DEFENSE INFORMATION SYSTEMS AGENCY
P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

Joint Interoperability Test Command (JTE)   **29 Nov 12**

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Joint Interoperability Certification of the Aruba Networks, Inc., 6000-400-F1, 6000-400-USF1 with M3mk1-S-F1Wireless Products with Software Release ArubaOS_MMC_6.1.4.0-FIPS

References: (a) Department of Defense Directive 4630.05, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," 5 May 2004
(b) Department of Defense Instruction 8100.04, "DoD Unified Capabilities (UC)," 9 December 2010
(c) through (e), see Enclosure 1

1. References (a) and (b) establish the Joint Interoperability Test Command (JITC) as the responsible organization for interoperability test certification.

2. The Aruba Networks, Inc. 6000-400-F1, 6000-400-USF1 with M3mk1-S-F1 Wireless Products with Software Release ArubaOS_MMC_6.1.4.0-FIPS, hereinafter referred to as the System Under Test (SUT), meet all critical interoperability requirements for Wireless Access Local Area Network (LAN) Systems (WLASs) and Wireless Access Bridges (WABs), and are certified for joint use in the Defense Information System Network. The United States Army Information Systems Engineering Command Technology Integration Center (USAISEC TIC) Fort Huachuca, Arizona, conducted Interoperability (IO) testing using wireless requirements derived from the "Unified Capabilities Requirements 2008 (UCR 2008), Change 3," Reference (c); and wireless test procedures, Reference (d). The JITC will verify the SUT's certification status during operational deployment and evaluate any new discrepancies noted in the operational environment for impact on the existing certification. These discrepancies will be adjudicated to the satisfaction of Defense Information Systems Agency (DISA) via a vendor Plan of Actions and Milestones that addresses all new critical Test Discrepancy Reports (TDRs) within 120 days of identification. No other configurations, features, or functions, except those cited within this memorandum, are certified by JITC or authorized by the Program Management Office for use. This certification expires upon changes that affect interoperability, but no later than three years from the date of this memorandum.

3. This certification finding is based on IO testing conducted by the USAISEC-TIC, review of the vendor's Letters of Compliance (LoCs), DISA adjudication of open TDRs and the DISA Certifying Authority (CA) Recommendation. The USAISEC-TIC, a Department of Defense (DoD) Component Test Lab, conducted IO testing from 14 May 2012 through 7 June 2012. Review of the vendor's LoCs was completed in May 2012. The test results for this product are published in a separate report, Reference (e). The DISA Information Assurance (IA) CA provided a positive recommendation on 24 October 2012, based on the security testing

JITC Memo, JTE, Joint Interoperability Certification of the Aruba Networks, Inc., 6000-400-F1, 6000-400-USF1 with M3mk1-S-F1 Wireless Products with Software Release ArubaOS_MMC_6.1.4.0-FIPS

completed by USAISEC-TIC-led IA test teams. JITC has reviewed the DoD component test lab results, Enclosure 2, and certifies the Aruba Networks, Inc. 6000-400-F1, 6000-400-USF1 with M3mk1-S-F1 Wireless Products with Software Release ArubaOS_MMC_6.1.4.0-FIPS as meeting the "UCR 2008, Change 3," requirements for WLAS and WAB. Enclosure 2 documents the test results and describes the tested network and system configurations.

4. The interface, Capability Requirements (CRs), Functional Requirements (FRs), and component status of the SUT are listed in Table 1. The threshold CR/FR for WLASs and WABs are established by Section 5.3.1 of Reference (c) and were used to evaluate the interoperability of the SUT.

Table 1. SUT Interface Interoperability Status

Interface	Critical (See note 1.)	UCR Reference	Threshold CR/FR Requirements (See note 2)	Status	Remarks
WLAS					
802.11a	N	5.3.1.7.2.3-1	1, 2, 3, 5, and 7	Certified	
802.11b	N	5.3.1.7.2.3-1	1, 2, 3, 5, and 7	Certified	
802.11g	N	5.3.1.7.2.3-1	1, 2, 3, 5, and 7	Certified	
802.11n	N	5.3.1.7.2.3-1	1, 2, 3, 5, and 7	Certified	
802.16	N	5.3.1.7.2.3-4	1, 2, 3, 5, and 7	N/A	
802.3i	N	5.3.1.7.2.5-5	1, 2, 3, 5, and 7	Certified	
802.3j	N	5.3.1.7.2.5-5	1, 2, 3, 5, and 7	Certified	See note 3.
802.3u	N	5.3.1.7.2.5-5	1, 2, 3, 5, and 7	Certified	
802.3 z	N	5.3.1.7.2.5-5	1, 2, 3, 5, and 7	Certified	See note 3.
802.3ab	N	5.3.1.7.2.5-5	1, 2, 3, 5, and 7	Certified	
WAB					
802.11a	N	5.3.1.7.2.6-1	1, 2, 3, 6, and 7	Certified	
802.11b	N	5.3.1.7.2.6-1	1, 2, 3, 6, and 7	Certified	
802.11g	N	5.3.1.7.2.6-1	1, 2, 3, 6, and 7	Certified	
802.11n	N	5.3.1.7.2.6-1	1, 2, 3, 6, and 7	Certified	
802.16	N	5.3.1.7.2.6-1	1, 2, 3, 6, and 7	N/A	
802.3i	N	5.3.1.7.2.6-1	1, 2, 3, 6, and 7	Certified	
802.3j	N	5.3.1.7.2.6-1	1, 2, 3, 6, and 7	Certified	See note 3.
802.3u	N	5.3.1.7.2.6-1	1, 2, 3, 6, and 7	Certified	
802.3z	N	5.3.1.7.2.6-1	1, 2, 3, 6, and 7	Certified	See note 3.
802.3ab	N	5.3.1.7.2.6-1	1, 2, 3, 6, and 7	Certified	
WEI					
802.11a	N	5.3.1.7.2.3	1, 3, and 4	N/A	Products tested did not include WEIs.
802.11b	N	5.3.1.7.2.3	1, 3, and 4	N/A	
802.11g	N	5.3.1.7.2.3	1, 3, and 4	N/A	
802.16	N	5.3.1.7.2.3	1, 3, and 4	N/A	

NOTES:
1. The "UCR 2008, Change 3," does not define any minimum interfaces. The SUT must minimally provide one of the wired interfaces (to the ASLAN) and wireless interfaces (subscriber).
2. The SUT need not provide wireless capabilities; however, if such capabilities are present, the SUT must meet all threshold CR/FR requirements. The detailed CRs/FRs are listed in Enclosure 3, System Capability Requirements and Functional Requirements.
3. Support for this interface type is through the use of an appropriate SFP installed at the controller.

Table 1. SUT Interface Interoperability Status (continued)

LEGEND:	
ASLAN Assured Services LAN	SFP Small Form-Factor Pluggable
CR Capability Requirement	SUT System Under Test
FR Functional Requirement	UCR Unified Capabilities Requirements
LAN Local Area Network	WAB Wireless Access Bridge
N No	WEI Wireless End Instrument
N/A Not Applicable	WLAS Wireless LAN Access System

Table 2. SUT Capability Requirements and Functional Requirements Status

CR/FR ID	Capability/Function	Applicability (See note 1)	UCR Reference	Status	Remarks
1	**General Wireless Requirements**				
	IPv6	Required	5.3.1.7.2.1	Met	See note 2.
	Wi-Fi Certified	Required (See note 3.)	5.3.1.7.2.1	Met	See note 4.
	Redundancy	Required	5.3.1.7.2.1	Met	
	FIPS 140-2 Level 1	Required	5.3.1.7.2.1	Met	See note 4.
	Latency	Required	5.3.1.7.2.1	Met	
	Traffic Prioritization	Required	5.3.1.7.2.1	Met	
	Wireless STIGs	Required	5.3.1.7.2.1	Met	See note 5.
	CAPWAP	Required	5.3.1.7.2.1	Partially Met	TDR issued See note 6.
2	**WIDS Requirements**				
	Continuous Scanning			Met	See note 7.
	Location-sensing			Met	See note 7.
3	**Wireless Interface Requirements**				
	Interface Standards	Required (See note 8.)	5.3.1.7.2.3	Met	
	802.11 Interface Standards	Required (See note 9.)	5.3.1.7.2.3	Met	
	802.16 Interface Standards	Required (See note 10.)	5.3.1.7.2.3	N/A	See note 11.
	Fixed/Nomadic WEIs	Required (See note 12.)	5.3.1.7.2.3	N/A	See note 13.
4	**WEI Requirements**				
	VoIP Solution	Required (See note 14.)	5.3.1.7.2.4	N/A	
	Access Methods	Required (See note 15.)	5.3.1.7.2.4	N/A	
	Call Control Authentication	Required (See note 14.)	5.3.1.7.2.4	N/A	
	Call Termination	Required (See note 12.)	5.3.1.7.2.4	N/A	
5	**WLAS Requirements**				
	Loss of Call upon WLAS failure	Required (See note 16.)	5.3.1.7.2.5	Met	See note 17.
	Maximum supported EIs	Required (See note 16.)	5.3.1.7.2.5	Met	See notes 17 and 18.
	MOS	Required (See note 16.)	5.3.1.7.2.5	Met	See notes 17 and 18.
	Roaming	Required (See note 16.)	5.3.1.7.2.5	Met	See note 17.

Table 2. SUT Capability Requirements and Functional Requirements Status

CR/FR ID	Capability/Function	Applicability (See note 1)	UCR Reference	Status	Remarks
6	**WAB Requirements**				
	Individual Interface Standards	Required (See note 9.)	5.3.1.7.2.6	Met	For specified interfaces.
	Maximum Voice Calls Transported	Required (See note 9.)	5.3.1.7.2.6	Met	See notes 17 and 18.
	Voice MOS	Required (See note 9.)	5.3.1.7.2.6	Met	See note 17.
	E2E BER	Required (See note 9.)	5.3.1.7.2.6	Met	
	Secure Voice Transmission	Required (See note 9.)	5.3.1.7.2.6	Met	See note 19.
	Call Signaling Transport	Required (See note 9.)	5.3.1.7.2.6	Met	See note 19.
	Latency	Required (See note 9.)	5.3.1.7.2.6	Met	
	Jitter	Required (See note 9.)	5.3.1.7.2.6	Met	TDR issued. See note 20.
	WLAS/WAB Combination	Required (See note 9.)	5.3.1.7.2.6	Met	
7	**ASLAN Requirements Applicable to Wireless Products**				
	General Performance Parameters	Required	5.3.1.3	Met	

NOTES:

1. The SUT need not provide wireless capability. However, if wireless capability is present, the SUT must meet the wireless requirements (as applicable for product type WLAS, WAB, or WEI) in order to be certified.
2. Vendor demonstrated IPv6 management and packet transfer via wireless and wired Ethernet.
3. Only applies to 802.11 interfaces.
4. Verified via vendor LoC and testing.
5. Vendor met STIG requirements with submitted mitigations.
6. The TDR was adjudicated by DISA on 10 July 2012, and was determined to be "Condition of Fielding" with operations limited to Aruba Wireless Controllers.
7. The SUT support WIDS extensive features of continuous scanning and location sensing.
8. Individual sub-requirements apply to specific interface types.
9. Applicable to 802.11 interfaces only.
10. Applicable to 802.16 interfaces only.
11. SUT does not provide 802.16 interface.
12. Applies to WEIs; not applicable to WLASs or WABs.
13. SUT does not include WEIs.
14. The WEI is certified in conjunction with a call-control agent (VoIP solution).
15. The WEI may be dedicated service (single traffic type) or shared service (voice, video, and data).
16. Specified requirements are only applicable to WLAS products.
17. Verified via emulated VoIP phone calls using test, measurement and diagnostic equipment.
18. The SUT was not tested to the maximum 96 EIs – see Testing Limitations in Enclosure 2.
19. No direct measurement available. Reference the SUT's demonstrated suitable quality wireless transport confirmed with collaborating measurements. The SUT is considered to meet this requirement with a low-risk assessment.
20. The TDR was adjudicated by DISA on 10 July 2012, and was determined to be "Change Requirement" from 1ms, allowing for 3 ms or less jitter.

JITC Memo, JTE, Joint Interoperability Certification of the Aruba Networks, Inc., 6000-400-F1, 6000-400-USF1 with M3mk1-S-F1 Wireless Products with Software Release ArubaOS_MMC_6.1.4.0-FIPS

Table 2. SUT Capability Requirements and Functional Requirements Status (continued)

LEGEND:			
802.11	IEEE Set of Wireless Standards in the 2.4,3.6, and 5 GHz	LoC	Letter of Compliance
802.16	IEEE Series of Wireless Broadband Standards	MOS	Mean Opinion Score
ASLAN	Assured Services LAN	ms	Millisecond
BER	Bit Error Rate	N/A	Not Applicable
CAPWAP	Control and Provisioning of Wireless Access Point	STIG	Security Technical Implementation Guide
DISA	Defense Information Systems Agency	SUT	System Under Test
CR	Capability Requirement	TDR	Test Discrepancy Report
E2E	End-to-End	UCR	Unified Capabilities Requirements
EI	End Instrument	WAB	Wireless Access Bridge
FIPS	Federal Information Processing Standard	WEI	Wireless End Instrument
FR	Functional Requirement	WIDS	Wireless Intrusion Detection System
GHz	Gigahertz	Wi-Fi	Trademark of the Wi-Fi Alliance that Refers to a Range of
ID	Identification		Connectivity Technologies Including WLAN
IEEE	Institute of Electrical and Electronics Engineers	WLAN	Wireless LAN
IPv6	Internet Protocol Version 6	WLAS	Wireless LAN Access System
LAN	Local Area Network	VoIP	Voice Over Internet Protocol

5. In accordance with the Program Manager's request, the JITC did not prepare a detailed test report. The JITC distributes interoperability information via the JITC Electronic Report Distribution system, which uses Non-secure Internet Protocol Router Network (NIPRNet) e-mail. More comprehensive interoperability status information is available via the JITC System Tracking Program (STP). The STP is accessible by .mil/gov users on the NIPRNet at https://stp.fhu.disa.mil. Test reports, lessons learned, and related testing documents and references are on the JITC Joint Interoperability Tool (JIT) at http://jit.fhu.disa.mil (NIPRNet). Information related to Defense Switched Network (DSN) testing is on the Telecom Switched Services Interoperability website at http://jitc.fhu.disa.mil/tssi. All associated data is available on the Defense Information Systems Agency Unified Capability Coordination Office (UCCO) website located at http://www.disa.mil/Services/Network-Services/UCCO.

6. The JITC point of contact is Lisa H. Fardsalehi, commercial 520-538-5531 or DSN 312-879-5531, e-mail: lisa.fardsalehi.civ@mail.mil. The JITC's mailing address is P.O. Box 12798, Fort Huachuca, AZ 85670-2798. The Defense Information Systems Agency (DISA) Unified Capability Coordination Office (UCCO) Tracking Number: 1134803.

FOR THE COMMANDER:

2 Enclosures a/s

BRADLEY A. CLARK
Acting Chief
Battlespace Communications Portfolio

JITC Memo, JTE, Joint Interoperability Certification of the Aruba Networks, Inc., 6000-400-F1, 6000-400-USF1 with M3mk1-S-F1 Wireless Products with Software Release ArubaOS_MMC_6.1.4.0-FIPS

Distribution (electronic mail):
Joint Staff J-6
Joint Interoperability Test Command, Liaison, TE3/JT1
Office of Chief of Naval Operations, CNO N6F2
Headquarters U.S. Air Force, Office of Warfighting Integration & CIO, AF/XCIN (A6N)
Department of the Army, Office of the Secretary of the Army, DA-OSA CIO/G-6 ASA (ALT), SAIS-IOQ
U.S. Marine Corps MARCORSYSCOM, SIAT, MJI Division I
DOT&E, Net-Centric Systems and Naval Warfare
U.S. Coast Guard, CG-64
Defense Intelligence Agency
National Security Agency, DT
Defense Information Systems Agency, TEMC
Office of Assistant Secretary of Defense (NII)/DoD CIO
U.S. Joint Forces Command, Net-Centric Integration, Communication, and Capabilities Division, J68
HQUSAISEC, AMSEL-IE-IS

ADDITIONAL REFERENCES

(c) Office of the Assistant Secretary of Defense, "Department of Defense Unified Capabilities Requirements 2008 (UCR 2008), Change 3," September 2011

(d) JITC "Unified Capabilities Test Plan (UCTP)," February 2012

(e) JITC, "Information Assurance (IA) Assessment" of Aruba Networks, Inc., 620-F1, 620-USF1, 650-F1, 650-USF1 ArubaOS_MMC_6.1.4.0-FIPS (UC TN 1134801), July 2012; Aruba Networks, Inc., 3200-F1, 3200-USF1, 3400-F1, 3400-USF1, 3600-F1, 3600-USF1 ArubaOS_MMC_6.1.4.0-FIPS (UC TN 1134802), July 2012; Aruba Networks, Inc., 6000-400-F1, 6000-400-USF1 with M3mk1-S-F1 ArubaOS_MMC_6.1.4.0-FIPS (UC TN 1134803), July 2012

(This page intentionally left blank.)

CERTIFICATION TESTING SUMMARY

1. SYSTEM TITLE. Aruba Networks, Inc., 6000-400-F1, 6000-400-USF1 with M3mk1-S-F1 ArubaOS_MMC_6.1.4.0-FIPS (UC TN 1134803), July 2012

2. SPONSOR. Mr. Steven Pursell, U.S. Army Information Systems Engineering Command (USAISEC), Technology Integration Center (TIC), Building 53302, Fort Huachuca, AZ 85613; e-mail: steven.d.pursell.civ@mail.mil

3. SYSTEM POINTS OF CONTACT. Mr. Barry Kroneberger; email: barry@arubanetworks.com, phone: (970) 531-2723

4. TESTER. Testing conducted at Department of Army Distributed Testing Lab, USAISEC-TIC, ATTN: James Hatch, Fort Huachuca, AZ 85613; e-mail: james.d.hatch12.civ@mail.mil

5. SYSTEM DESCRIPTION.

    a. General Description. Aruba Networks provides enterprise mobility Wireless Access Local Area Network (LAN) Systems (WLAS) and Wireless Access Bridges (WAB) solutions enabling secure access to data, voice, and video applications across wireless and wired enterprise networks. Wireless transport is protected by the use of Wireless Protected Access 2 Enterprise (WPA2-Enterprise) with the Advanced Encryption Standard (AES) encryption algorithm. Management sessions are secured using Transport Layer Security (TLS) or Secure Shell (SSH) with Federal Information Processing Standard (FIPS) validated algorithms. For this evaluation, the system under test (SUT) consisted of the following components:

        (1) Controllers: Aruba Networks Mobility Controller 650, 3400, and 6000-400 chassis with M3mk1-S multi-service controller module.

        (2) Access Points (APs): Remote Access Point (RAP)-5WN, AP-93, AP-105, AP-125, AP-135, and AP-175.

    b. Management Description. The Aruba Networks family of wireless controllers, 600, 3000, and 6000 series, are accessed in two phases: initialization and deployed. At the initialization phase, a management workstation may use the controller's serial console interface or use the WebGUI (Graphical User Interface) to access the controller's startup script for basic configuration options (Internet Protocol [IP] address, subnet mask, default gateway, master/local controller, initial time, initial admin and enable passwords, country code, etc.). In the second phase, deployed configuration management sessions to a controller use HyperText Transfer Protocol Secure (HTTPS) for an encrypted session to the WebGUI. The alternative is a SSH management session to the controller's Command Line Interface (CLI).

For the GUI, Aruba implements an Apache web server which enables system

administrators to fully manage the controller platforms from a standard web browser.

This FIPS version of controller software constrains all management sessions to use only approved secure management modes. System administrators may manage the system using either the CLI or GUI. Comprehensive administrative functions are available in each mode, to include general network settings, user and administrative profile management, monitoring wireless operations status and alarm conditions, managing APs, channel utilization, and performing system-wide maintenance.

After the initial system configuration, administrators will provision wireless users' authentication and authorization using multi-part credentials comprised of authorized digital certificates and passphrases. Users seeking wireless authentication and authorization are challenged by the wireless controller and remotely authenticated by a networked Remote Authentication Dial-In User Service (RADIUS) server. Wireless controllers' administrators will be authenticated via an Lightweight Directory Access Protocol (LDAP)* server using LDAP over Secure Sockets Layer [SSL] (LDAPS). Besides username/password authentication, administrator accounts can be configured to use certificate-based authentication using a Common Access Card (CAC). During the evaluation, only locally configured administrator accounts were able to log in successfully using CAC. Active Directory (AD) integrated administrator accounts were not able to log in using certificate-based authentication.

*Note: The same RADIUS server used for client authentication cannot be used for administrator authentication. This is because the controllers only support the Password Authentication Protocol (PAP) for administrator authentication. Since PAP is not an acceptable authentication method, the controllers must use an LDAP server via LDAPS, which provides a secure method for administrator authentication.

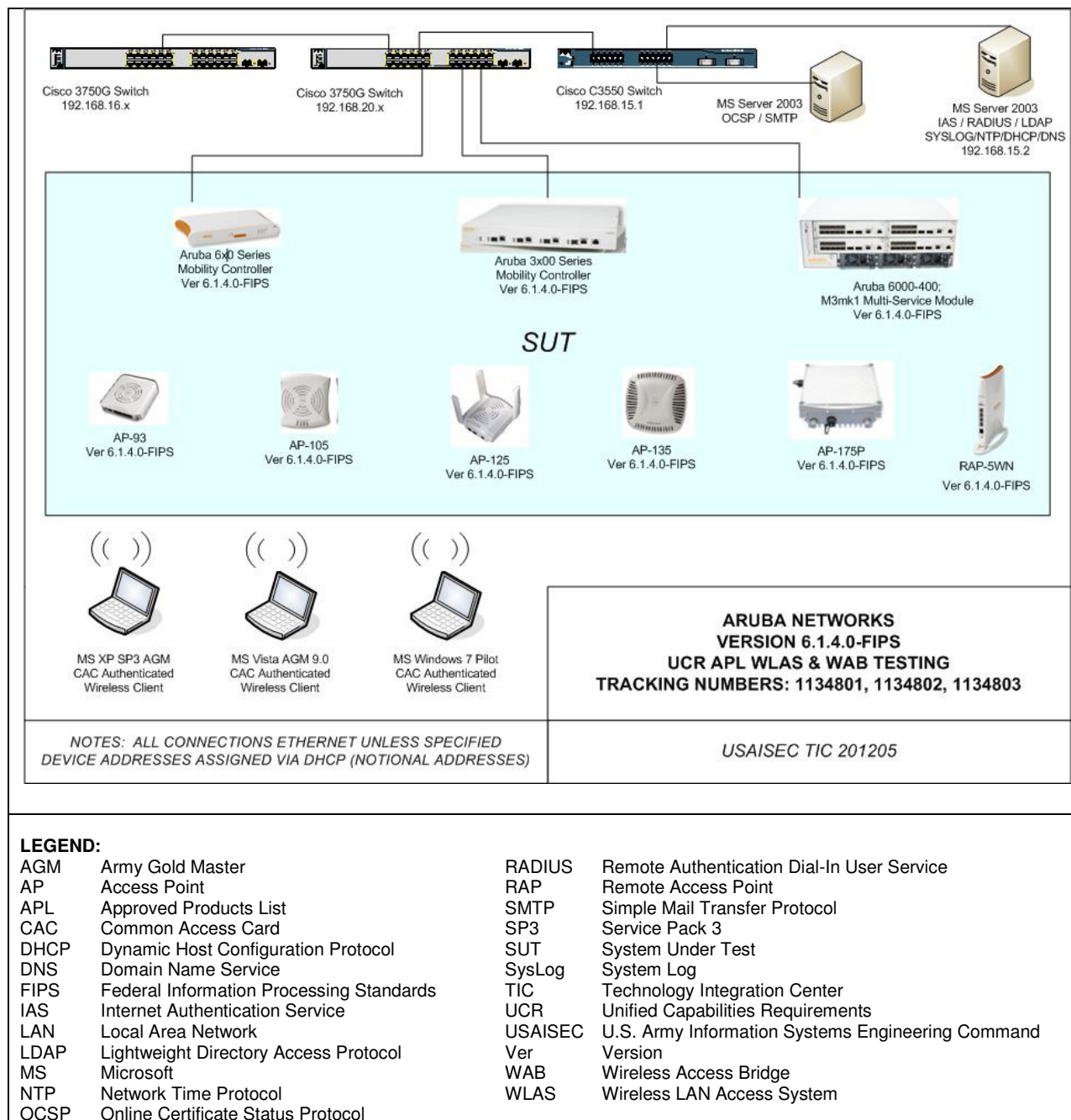   **c. Components Under Test.** Figure 2-1 depicts the system; descriptions of the components follow.

Figure 2-1. Architecture – System Under Test

LEGEND:

AGM	Army Gold Master	RADIUS	Remote Authentication Dial-In User Service
AP	Access Point	RAP	Remote Access Point
APL	Approved Products List	SMTP	Simple Mail Transfer Protocol
CAC	Common Access Card	SP3	Service Pack 3
DHCP	Dynamic Host Configuration Protocol	SUT	System Under Test
DNS	Domain Name Service	SysLog	System Log
FIPS	Federal Information Processing Standards	TIC	Technology Integration Center
IAS	Internet Authentication Service	UCR	Unified Capabilities Requirements
LAN	Local Area Network	USAISEC	U.S. Army Information Systems Engineering Command
LDAP	Lightweight Directory Access Protocol	Ver	Version
MS	Microsoft	WAB	Wireless Access Bridge
NTP	Network Time Protocol	WLAS	Wireless LAN Access System
OCSP	Online Certificate Status Protocol		

    (1) **Aruba Networks 6x0 Series Controller.** This controller can aggregate up to 8 (620 controller) or 16 (650 controller) LAN-connected APs. Aruba wireless controllers separate the higher layer security and service delivery from the network transport functions. This architecture uses the separation of functions extending to the Aruba APs, which move user traffic to the controller via secure tunnels while retaining all management functions at the controller. The Aruba APs are initially unmanaged, containing no configuration until they are administratively associated to a controller.

Upon AP association to the controller, the AP is provisioned with the appropriate configuration and firmware supporting secure tunneling of user data to the controller.

The fixed configuration of the 620 chassis consists of one 10/100/1000Base-T Ethernet port, eight 10/100Base-T Ethernet ports, one registered jack-45 (RJ-45) serial console port, four universal serial bus (USB) 2.0 type A ports, and one ExpressCard slot.

The fixed configuration of the 650 chassis consists of two 1000Base-X small form-factor pluggable (SFP) ports, six 10/100/1000Base-T Ethernet ports (four ports support 802.3af Power over Ethernet [PoE]), one RJ-45 serial console port, one USB 2.0 type A port, and one ExpressCard slot.

       (2) Aruba Networks 3x00 Controller. This controller can aggregate up to 32 (3200 controller), 64 (3400 controller), or 128 (3600 controller) LAN-connected APs. Aruba wireless controllers separate the higher layer security and service delivery from the network transport functions. This architecture uses the separation of functions extending to the Aruba APs, which move user traffic to the controller via secure tunnels while retaining all management functions at the controller. The Aruba APs are initially unmanaged, containing no configuration until they are administratively associated to a controller. Upon AP association to the controller, the AP is provisioned with the appropriate configuration and firmware supporting secure tunneling of user data to the controller.

The fixed configuration of the chassis consists of four dual-media 10/100/1000Base-T or 1000Base-X (SFP) ports and one RJ-45 serial console port.

       (3) Aruba Networks 6000-400 Controller. This controller aggregates up to 2,048 APs (512 APs per M3 Mark 1 module) in a single chassis with two 400 Watt (W) power supplies. Aruba wireless controllers separate the higher layer security and service delivery from the network transport functions. This architecture uses the separation of functions extending to the Aruba APs, which move user traffic to the controller via secure tunnels while retaining all management functions at the controller. The Aruba APs are initially unmanaged, containing no configuration until they are administratively associated to a controller. Upon AP association to the controller, the AP is provisioned with the appropriate configuration and firmware supporting secure tunneling of user data to the controller.

The chassis has four slots that support one or more M3 Mark 1 card.

       • **Card 1:** The Multi-Service Mobility Module Mark 1 (M3 Mark 1/M3mk1) module provides 20 Gigabits per second (Gbps) throughput and supports 512 LAN-connected APs. The card includes two (2) 10GBase-X 10 Gigabit SFP ports, ten (10) 1000Base-X SFP ports, one (1) 10/100/1000Base-T Ethernet management port, and one (1) RJ-45 serial console port.

(4) Aruba Networks AP-93 and AP-92*. This wireless AP is indoor rated and has a single dual-band radio (Institute of Electrical and Electronics Engineers [IEEE] 802.11 a/n + 802.11 b/g/n, single-band selectable) using two omni-directional integrated antennas. The AP-93 can be used for wireless access, intrusion detection monitoring, traffic analysis, or remote AP applications across the 2.4 Gigahertz (GHz) or 5 GHz radio frequency (RF) spectrums. It supports 2x2 Multiple-In Multiple-Out (MIMO), one 10/100/1000Base-T Ethernet port, one RJ-45 serial console interface, backward compatibility with IEEE 802.11a/b/g, and IEEE 802.11n. It is powered using standard IEEE 802.3af PoE.

*Note: The AP-92 is internally identical to the AP-93. The variance is external antenna support via two external RF connectors, RP-SubMiniature A Connector (SMA) type. Please refer to a similar citation in the related Interoperability (IO) Test Report.

(5) Aruba Networks AP-105 and AP-104*. This wireless AP is indoor rated and has two dual-band radios (dual-band concurrent IEEE 802.11 a/n + 802.11 b/g/n) using two omni-directional integrated antennas. The AP-105 can be used for wireless access, intrusion detection monitoring, traffic analysis, or remote AP applications across the 2.4 GHz and 5 GHz RF spectrums. It supports 2x2 MIMO, one 10/100/1000Base-T Ethernet port, one RJ-45 serial console interface, backward compatibility with IEEE 802.11a/b/g, and IEEE 802.11n. It is powered using standard IEEE 802.3af PoE.

*Note: The AP-104 is internally identical to the AP-105. The variance is external antenna support via two external RF connectors, RP-SMA type. Please refer to a similar citation in the related IO Test Report.

(6) Aruba Networks AP-125 and AP-124*. This wireless AP is indoor rated and has two dual-band radios (dual-band concurrent IEEE 802.11 a/n + 802.11 b/g/n) using three omni-directional integrated antennas. The AP-125 can be used for wireless access, intrusion detection monitoring, traffic analysis, or remote AP applications across the 2.4 GHz and 5 GHz RF spectrums. It supports 3x3 MIMO with two spatial streams, dual 10/100/1000Base-T Ethernet ports, one RJ-45 serial console interface, backward compatibility with IEEE 802.11a/b/g, and combined IEEE 802.11n. It is powered using standard IEEE 802.3af or IEEE 802.3at PoE.

*Note: The AP-124 is internally identical to the AP-125. The variance is external antenna support via three external RF connectors, RP-SMA type. Please refer to a similar citation in the related IO Test Report.

(7) Aruba Networks AP-135 and AP-134*. This wireless AP is indoor rated and has two dual-band radios (dual-band concurrent IEEE 802.11 a/n + 802.11 b/g/n) using three downtilt omni-directional integrated antennas. The AP-135 can be used for wireless access, intrusion detection monitoring, traffic analysis, or remote AP applications across the 2.4 GHz and 5 GHz RF spectrums. It supports 3x3 MIMO with three spatial streams, dual 10/100/1000Base-T Ethernet ports, one RJ-45 serial console interface, backward compatibility with IEEE 802.11a/b/g, and combined IEEE 802.11n. It is powered using standard IEEE 802.3af or IEEE 802.3at PoE.

*Note: The AP-134 is internally identical to the AP-135. The variance is external antenna support via two external RF connectors, RP-SMA type. Please refer to a similar citation in the related IO Test Report.

      (8) Aruba Networks AP-175P, AP-175AC, and AP-175DC*. This wireless AP is a hardened, outdoor rated, dual radio (dual-band concurrent IEEE 802.11 a/n + 802.11 b/g/n) wireless AP with 4 N-type antenna interfaces (two each per band). It is capable of supporting multiple functions across the 2.4 GHz and 5 GHz RF spectrums, including wireless LAN (WLAN) client access, air monitoring/wireless intrusion detection and prevention, secure outdoor mesh, and bridging. The AP-175 operates on standard 802.3at PoE+, 100-240 volt alternating current (AC), or 12-48 volt direct current (DC), depending on the AP model*. It supports 2x2 MIMO with two spatial streams, one 10/100/1000Base-T Ethernet port, and one USB console port.

*Note: The AP-175 models are identical except for supporting different types of power in. The AP-175P requires 802.3at PoE+. The AP-175AC requires 100-240 volt AC from an external AC source. The AP-175DC requires 12-48 volt DC from an external DC power source.

      (9) Aruba Networks RAP-5WN. This wireless AP is indoor rated and has a single dual-band radio (IEEE 802.11 a/n + 802.11 b/g/n, single-band selectable) using three omni-directional integrated antennas. The RAP-5WN can be used for wireless access, intrusion detection monitoring, traffic analysis, or remote branch office/teleworker applications across the 2.4 GHz or 5 GHz RF spectrums. It supports 3x3 MIMO with two spatial streams, one 10/100/1000Base-T Ethernet port, four 10/100Base-T Ethernet ports, and one USB 2.0 type A port. It is powered with 12 volt DC using the included 100-240 volt AC to DC adapter.

6. OPERATIONAL ARCHITECTURE. The Defense Information System Network (DISN) architecture consists of DoD backbone and Service/Agency installation switches. The Camp/Post/Station architecture includes Assured Services Local Area Network (ASLAN) components. The Wireless Products extend ASLAN Services to wireless users. Figure 2-2 depicts the Operational Architecture and the relationship of the Wireless Products.
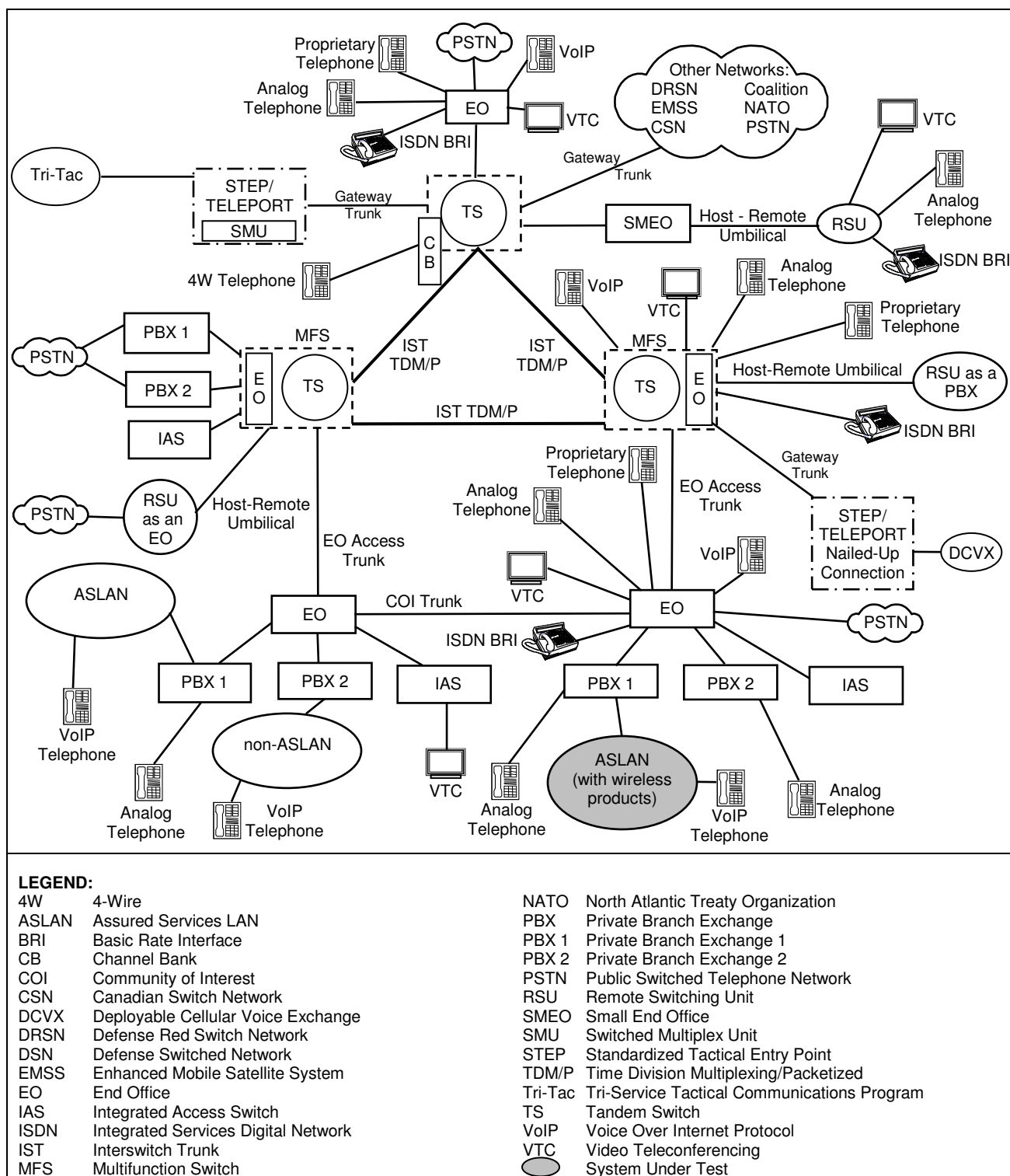
Figure 2-2. Operational Architecture

LEGEND:

4W	4-Wire	NATO	North Atlantic Treaty Organization
ASLAN	Assured Services LAN	PBX	Private Branch Exchange
BRI	Basic Rate Interface	PBX 1	Private Branch Exchange 1
CB	Channel Bank	PBX 2	Private Branch Exchange 2
COI	Community of Interest	PSTN	Public Switched Telephone Network
CSN	Canadian Switch Network	RSU	Remote Switching Unit
DCVX	Deployable Cellular Voice Exchange	SMEO	Small End Office
DRSN	Defense Red Switch Network	SMU	Switched Multiplex Unit
DSN	Defense Switched Network	STEP	Standardized Tactical Entry Point
EMSS	Enhanced Mobile Satellite System	TDM/P	Time Division Multiplexing/Packetized
EO	End Office	Tri-Tac	Tri-Service Tactical Communications Program
IAS	Integrated Access Switch	TS	Tandem Switch
ISDN	Integrated Services Digital Network	VoIP	Voice Over Internet Protocol
IST	Interswitch Trunk	VTC	Video Teleconferencing
MFS	Multifunction Switch		System Under Test

7. INTEROPERABILITY REQUIREMENTS. The interface, Capability Requirements (CRs), Functional Requirements (FRs), Information Assurance (IA), and other requirements for wireless products are established by Section 5.3.1 of the Department of Defense (DoD) "Unified Capabilities Requirements 2008 (UCR 2008), Change 3."

7.1 Interfaces. The wireless products use its interfaces to connect to the Assured Services [LAN] Local Area Network (ASLAN) infrastructure and wireless devices (voice, video, and data). The threshold requirements for interfaces specific to the wireless products are listed in Table 2-1.

Table 2-1. Wireless Interface Requirements

Interface	Critical (See note 1.)	UCR Reference	Threshold CR/FR Requirements (See note 2.)	Criteria	Remarks
WLAS					
802.11a	N	5.3.1.7.2.3	1, 2, 3, and 5	Meet minimum CR/FRs and 802.11 interface standards.	Provides wireless subscriber access.
802.11b	N	5.3.1.7.2.3	1, 2, 3, and 5		
802.11g	N	5.3.1.7.2.3	1, 2, 3, and 5		
802.16	N	5.3.1.7.2.3	1, 2, 3, and 5	Meet minimum CR/FRs and 802.16 interface standards.	Provides wireless subscriber access.
802.3i	N	5.3.1	1, 2, 3, and 5	Meet minimum CR/FRs and 802.3 interface standards.	Provides wired ASLAN access and NM interface.
802.3u	N	5.3.1	1, 2, 3, and 5		
802.3 z	N	5.3.1	1, 2, 3, and 5		
802.3ab	N	5.3.1	1, 2, 3, and 5		
WAB					
802.11a	N	5.3.1.7.2.3	1, 2, 3, and 6	Meet minimum CR/FRs and 802.11 interface standards.	Provides wireless subscriber access.
802.11b	N	5.3.1.7.2.3	1, 2, 3, and 6		
802.11g	N	5.3.1.7.2.3	1, 2, 3, and 6		
802.16	N	5.3.1.7.2.3	1, 2, 3, and 6	Meet minimum CR/FRs and 802.16 interface standards.	Provides wireless subscriber access.
802.3i	N	5.3.1	1, 2, 3, and 6	Meet minimum CR/FRs and 802.3 interface standards.	Provides wired ASLAN access and NM interface.
802.3u	N	5.3.1	1, 2, 3, and 6		
802.3z	N	5.3.1	1, 2, 3, and 6		
802.3ab	N	5.3.1	1, 2, 3, and 6		
WEI					
802.11a	N	5.3.1.7.2.3	1, 3, and 4	Meet minimum CR/FRs and 802.11 interface standards.	Provides wireless subscriber access.
802.11b	N	5.3.1.7.2.3	1, 3, and 4		
802.11g	N	5.3.1.7.2.3	1, 3, and 4		
802.16	N	5.3.1.7.2.3	1, 3, and 4	Meet minimum CR/FRs and 802.16 interface standards.	Provides wireless subscriber access.

NOTES:
1. "Required definition" means "conditionally required." The SUT need not provide wireless capabilities; however, if such capabilities are present, the SUT must meet all threshold CRs/FRs.
2. The detailed CRs/FRs are listed in Enclosure 3, System Capability Requirements and Functional Requirements.
3. These CR/FRs are not specific to any of the interfaces; however, the SUT must demonstrate the requirements in order to be certified.
4. The "UCR 2008, Change 3," references for each CR/FR are listed in Enclosure 3.

7.2 Capability Requirements and Functional Requirements. Wireless products have required and conditional features and capabilities that are established by Section 5.3.1.7.2 of the "UCR 2008**,** Change 3." The SUT does not need to provide non-critical (conditional) features and capabilities. If they are present, however, they must function according to the specified requirements. The features and capabilities and their associated requirements for wireless products are listed in Table 2-2. Detailed CR/FR requirements are provided in Table 3-1 of the System Capability Requirements and Functional Requirements.

Table 2-2. Wireless Capability Requirements and Functional Requirements

CR/FR ID	Capability/Function	Applicability (See note 1.)	UCR Reference	Criteria	Remarks
	General Wireless Requirements				
1	IPv6	Required	5.3.1.7.2.1	Meet applicable "UCR 2008**,** Change 3*,"* requirements. Detailed requirements and associated criteria are provided in Table 3-1 of Enclosure 3.	Applicability per product type (WLAS, WAB, or WEI) is provided in Table 3-1 of Enclosure 3.
	Wi-Fi Certified	Required (See note 2.)	5.3.1.7.2.1		
	Redundancy	Required	5.3.1.7.2.1		
	FIPS 140-2 Level 1	Required	5.3.1.7.2.1		
	Latency	Required	5.3.1.7.2.1		
	Traffic Prioritization	Required	5.3.1.7.2.1		
	Wireless STIGs	Required	5.3.1.7.2.1		
	CAPWAP	Required	5.3.1.7.2.1		
	WIDS				
2	Continuous Scanning			See Table 3-1 of Enclosure 3.	Applies to WLAS and WAB products.
	Location-sensing				
	Wireless Interface Requirements				
3	Interface Standards	Required (See note 3.)	5.3.1.7.2.3	Meet applicable "UCR 2008**,** Change 3*,"* requirements. Detailed requirements and associated criteria are provided in Table 3-1 of Enclosure 3.	Applicability per product type (WLAS, WAB, or WEI) is provided in Table 3-1 of Enclosure 3.
	802.11 Interface Standards	Required (See note 4.)	5.3.1.7.2.3		
	802.16 Interface Standards	Required (See note 5.)	5.3.1.7.2.3		
	Fixed/Nomadic WEIs	Required (See note 6.)	5.3.1.7.2.3		
	Wireless End Instruments				
4	VoIP Solution	Required (See note 7.)	5.3.1.7.2.4	Meet applicable "UCR 2008**,** Change 3*,"* requirements. Detailed requirements and associated criteria are provided in Table 3-1 of Enclosure 3.	Applicability per product type (WLAS, WAB, or WEI) is provided in Table 3-1 of Enclosure 3.
	Access Methods	Required (See note 8.)	5.3.1.7.2.4		
	Call Control Authentication	Required (See note 6.)	5.3.1.7.2.4		
	Call Termination	Required (See note 6.)	5.3.1.7.2.4		

Table 2-2. Wireless Capability Requirements and Functional Requirements (continued)

CR/FR ID	Capability/Function	Applicability (See note 1.)	UCR Reference	Criteria	Remarks
	WLAS Requirements				
5	Loss of Call upon WLAS failure	Required (See note 7.)	5.3.1.7.2.5	Meet applicable "UCR 2008, Change 3," requirements. Detailed requirements and associated criteria are provided in Table 3-1 of Enclosure 3.	Applies to WLAS only.
	Maximum supported EIs	Required (See note 7.)	5.3.1.7.2.5		
	MOS	Required (See note 7.)	5.3.1.7.2.5		
	Roaming	Required (See note 7.)	5.3.1.7.2.5		
	Wireless Access Bridge				
6	Individual Interface Standards	Required (See note 8.)	5.3.1.7.2.6	Meet applicable "UCR 2008, Change 3," requirements. Detailed requirements and associated criteria are provided in Table 3-1 of Enclosure 3.	Applies to WAB only.
	Maximum Voice Calls Transported	Required (See note 8.)	5.3.1.7.2.6		
	Voice MOS	Required (See note 8.)	5.3.1.7.2.6		
	E2E BER	Required (See note 8.)	5.3.1.7.2.6		
	Secure Voice Transmission	Required (See note 8.)	5.3.1.7.2.6		
	Call Signaling Transport	Required (See note 8.)	5.3.1.7.2.6		
	Latency	Required (See note 8.)	5.3.1.7.2.6		
	Jitter	Required (See note 8.)	5.3.1.7.2.6		
	WLAS/WAB Combination	Required (See note 8.)	5.3.1.7.2.6		
	ASLAN Requirements Applicable to Wireless Products				
7	General Performance Parameters	Required	5.3.1.3	See Table 3-1 of Enclosure 3.	

NOTES:
1. The SUT need not provide wireless capability. However, if wireless capability is present, the SUT must meet the wireless requirements (as applicable for product type WLAS, WAB, or WEI) in order to be certified.
2. Only applies to 802.11 interfaces.
3. Individual sub-requirements apply to specific interface types.
4. Applicable to 802.11 interfaces only.
5. Applicable to 802.16 interfaces only.
6. Applies to WEIs; not applicable to WLASs or WABs.
7. The WEI is certified in conjunction with a call-control agent (VoIP solution).
8. The WEI may be dedicated service (single traffic type) or shared service (voice, video, and data).

LEGEND:

802.11	IEEE Set of Wireless Standards in the 2.4,3.6, and 5 GHz	LAN	Local Area Network
802.16	IEEE Series of Wireless Broadband Standards	MOS	Mean Opinion Score
ASLAN	Assured Services LAN	STIG	Security Technical Implementation Guide
BER	Bit Error Rate	SUT	System Under Test
CAPWAP	Control and Provisioning of Wireless Access Point	UCR	Unified Capabilities Requirements
CR	Capability Requirement	WAB	Wireless Access Bridge
E2E	End-to-End	WEI	Wireless End Instrument
EIs	End Instruments	WIDS	Wireless Intrusion Detection System
FIPS	Federal Information Processing Standard	Wi-Fi	Trademark of the Wi-Fi Alliance that Refers to a Range of Connectivity Technologies Including WLAN
FR	Functional Requirement		
GHz	Gigahertz	WLAN	Wireless LAN
ID	Identification	WLAS	Wireless LAN Access System
IEEE	Institute of Electrical and Electronics Engineers	VoIP	Voice Over Internet Protocol
IPv6	Internet Protocol Version 6		

7.3 Information Assurance. The IA requirements for wireless products are listed in Table 2-3. The IA requirements were derived from Section 5.3.1 of the "UCR 2008**,** Change 3," "ASLAN Infrastructure;" and Section 5.4, "Information Assurance Requirements."

Table 2-3. Wireless IA Requirements

Requirement	Critical (See note)	UCR Reference
Wi-Fi Alliance Certified (802.11 only)	Yes	5.3.1.7.2.1
FIPS 140-2 Level 1/2	Yes	5.3.1.7.2.1
Wireless STIG Requirements	Yes	5.3.1.7.2.1
WIDS Monitoring		
General Requirements	Yes	5.4.6.2
Authentication	Yes	5.4.6.2.1
Integrity	Yes	5.4.6.2.2
Confidentiality	Yes	5.4.6.2.3
Non-repudiation	Yes	5.4.6.2.4
Availability	Yes	5.4.6.2.5

NOTE: Not all IA requirements from the referenced "UCR 2008**,** Change 3*,"* section apply. Refer to Table 1 of the System Capability Requirements and Functional Requirements for the specific IA requirements.

LEGEND:
FIPS   Federal Information Processing Standard   UCR   Unified Capabilities Requirements
IA   Information Assurance   WIDS   Wireless Intrusion Detection System
STIG   Secure Technical Implementation Guide   Wi-Fi   Wireless Fidelity, IEEE Series of Wireless Standards

7.4 Other. None.

8. TEST NETWORK DESCRIPTION. The SUT was tested at the USAISEC-TIC in a manner and configuration similar to that of the DISN operational environment. Testing of the system's required functions and features was conducted using the test configurations depicted in Figures 2-3 through 2-6.
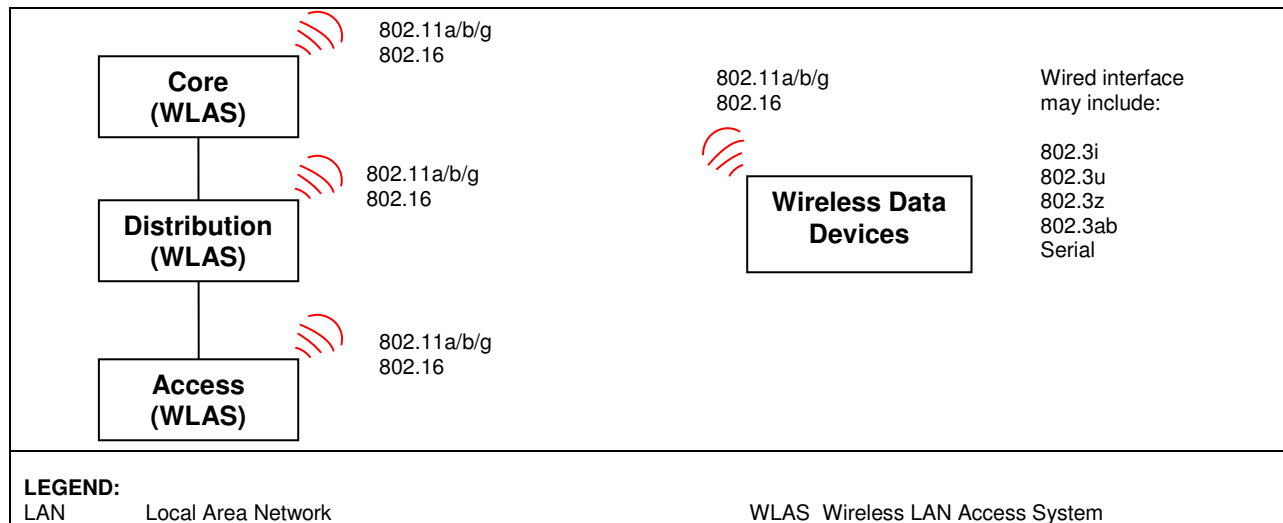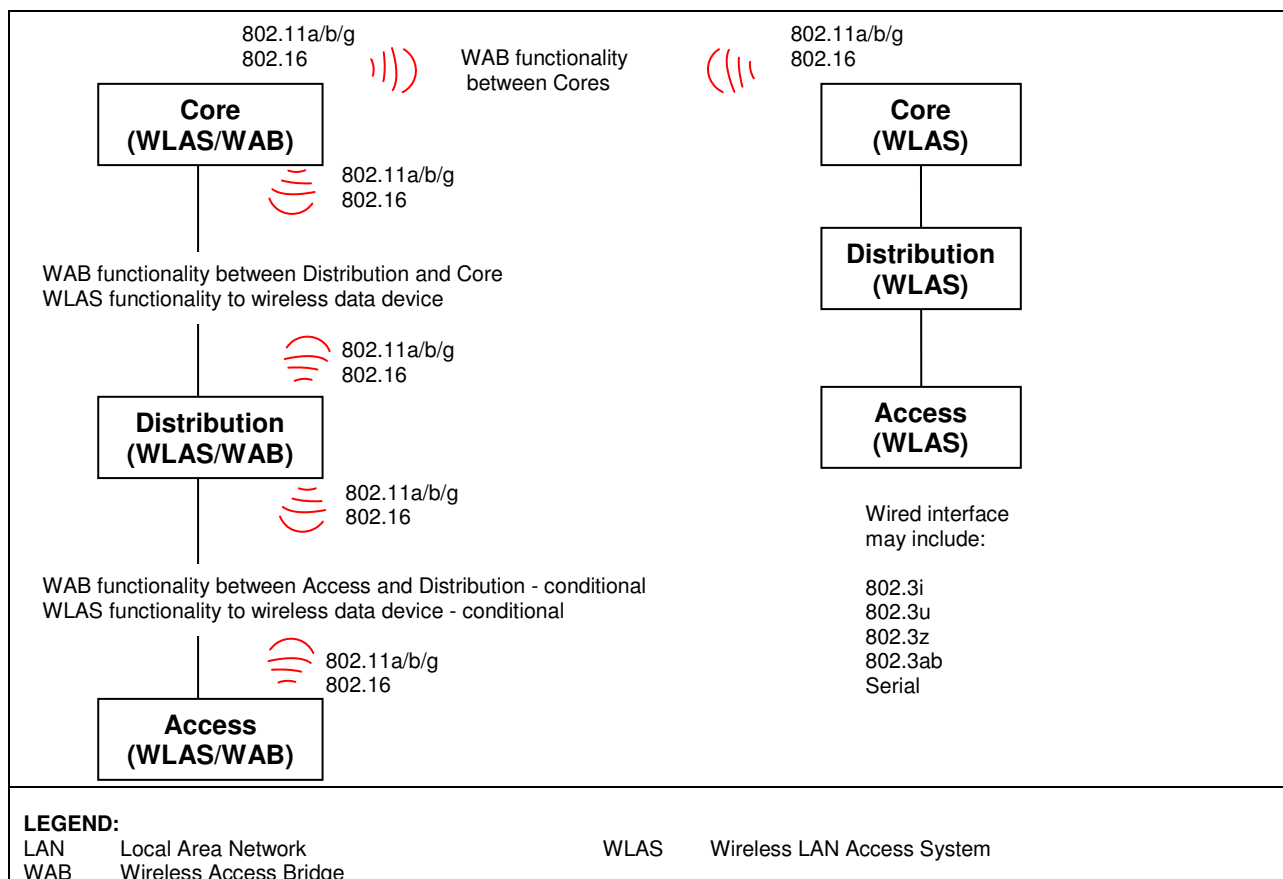
Figure 2-3. WLAS Test Configuration
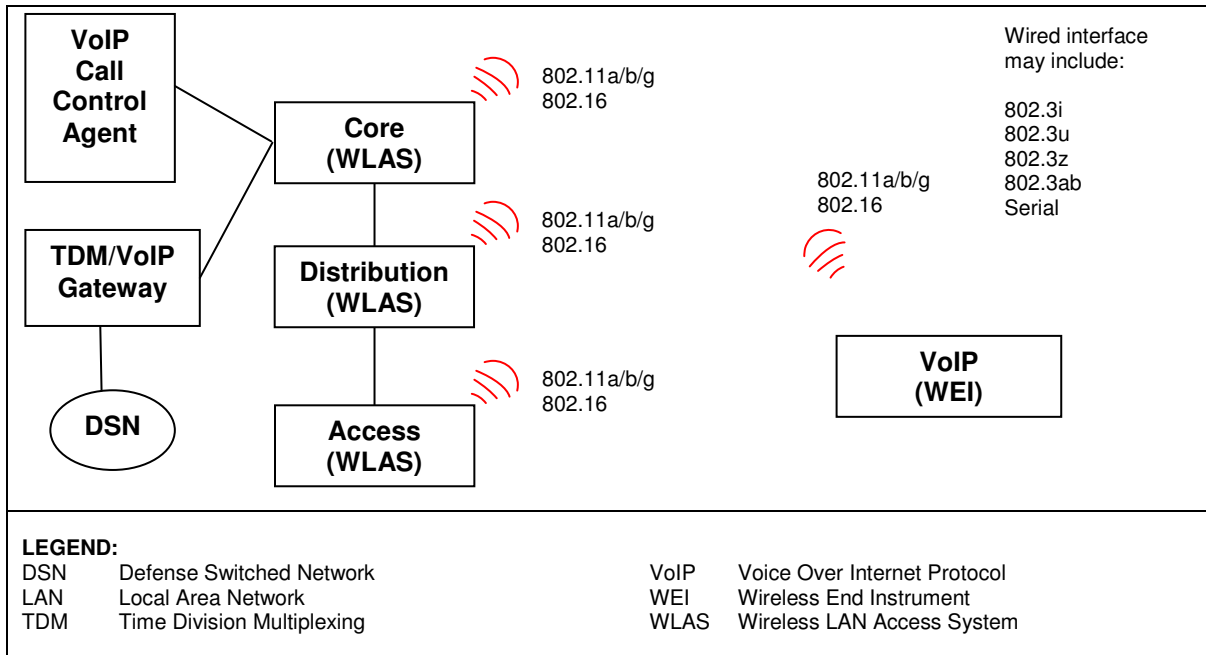

Figure 2-4. WAB Test Configuration
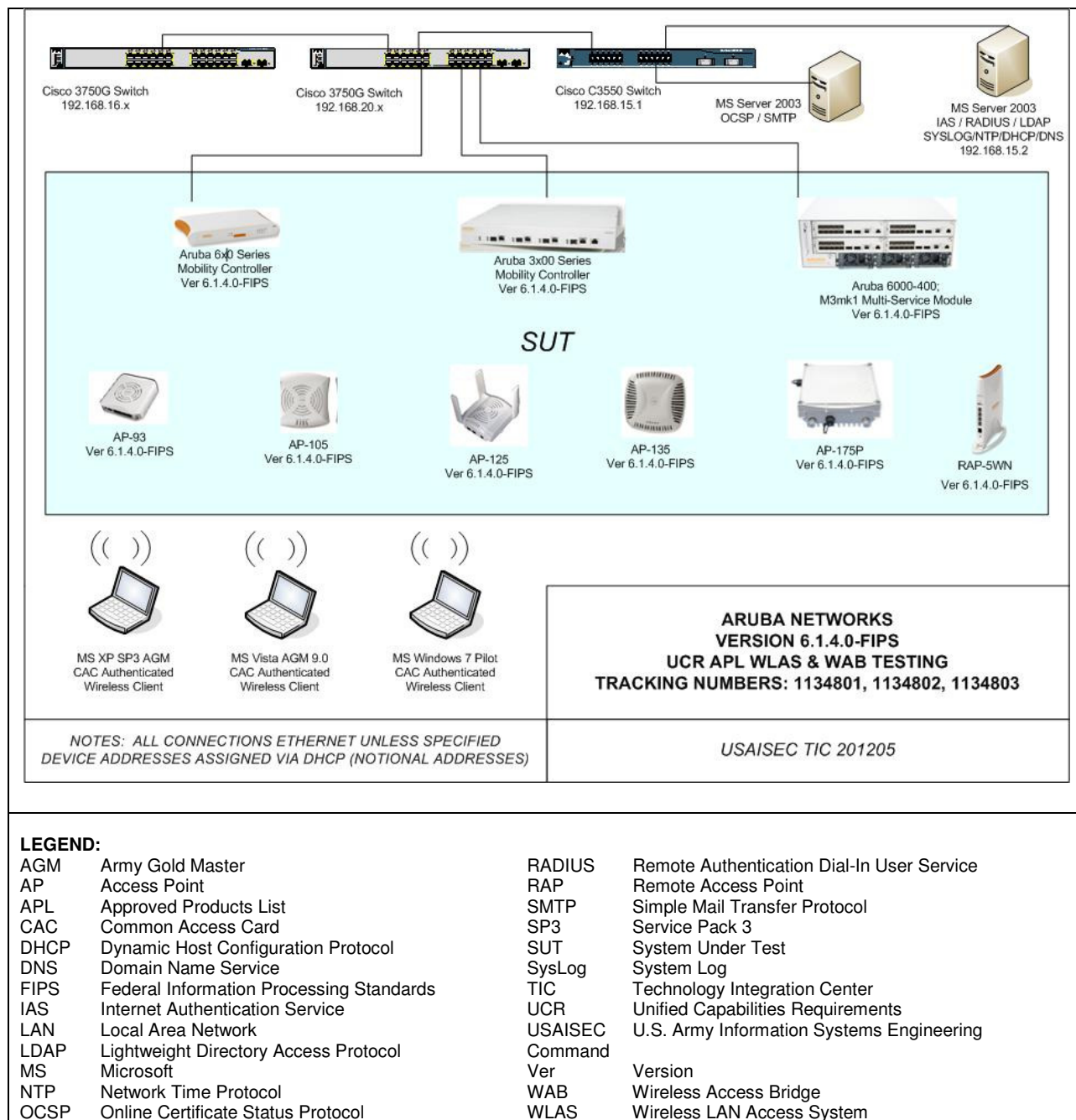
Figure 2-5. WEI Test Configuration

LEGEND:

AGM	Army Gold Master	RADIUS	Remote Authentication Dial-In User Service
AP	Access Point	RAP	Remote Access Point
APL	Approved Products List	SMTP	Simple Mail Transfer Protocol
CAC	Common Access Card	SP3	Service Pack 3
DHCP	Dynamic Host Configuration Protocol	SUT	System Under Test
DNS	Domain Name Service	SysLog	System Log
FIPS	Federal Information Processing Standards	TIC	Technology Integration Center
IAS	Internet Authentication Service	UCR	Unified Capabilities Requirements
LAN	Local Area Network	USAISEC	U.S. Army Information Systems Engineering
LDAP	Lightweight Directory Access Protocol	Command	
MS	Microsoft	Ver	Version
NTP	Network Time Protocol	WAB	Wireless Access Bridge
OCSP	Online Certificate Status Protocol	WLAS	Wireless LAN Access System

Figure 2-6. Wireless Test Configuration

9. SYSTEM CONFIGURATIONS. Table 2-4 provides the system configurations and hardware and software components tested with the SUT. The SUT was tested in an operationally realistic environment to determine interoperability with a complement of ASLAN Infrastructure products. The ASLAN infrastructure products listed are those used in the tested configuration. The list is not intended to identify only those ASLAN infrastructure products that are certified for use with the SUT. The SUT is certified for use with any/all of the ASLAN infrastructure products on the Unified Capabilities (UC) Approved Products List (APL).

Table 2-4. Tested System Configurations

System Name	Equipment		
Required Ancillary Equipment	Active Directory		
	PKI		
	RADIUS		
	SysLog Server		
Additional Equipment Needed	Management Workstation		
	LDAP Server		
	Hardware	**Cards**	**Software/Firmware**
	Aruba Networks 620 Controller	N/A	6.1.4.0-FIPS
	Aruba Networks **650 Controller**	N/A	6.1.4.0-FIPS
	Aruba Networks 3200 Controller	N/A	6.1.4.0-FIPS
	Aruba Networks **3400 Controller**	N/A	6.1.4.0-FIPS
	Aruba Networks **6000 Controller**	**M3mk1-S-F1**	6.1.4.0-FIPS
Aruba Networks, Inc., 6000-400-F1, 6000-400-USF1 with M3mk1-S-F1 (UC TN 1134803)	Aruba Networks AP-92	N/A	6.1.4.0-FIPS
	Aruba Networks **AP-93**	N/A	6.1.4.0-FIPS
	Aruba Networks AP-104	N/A	6.1.4.0-FIPS
	Aruba Networks **AP-105**	N/A	6.1.4.0-FIPS
(Bolded and Underlined hardware items are devices included in actual testing.)	Aruba Networks AP-124	N/A	6.1.4.0-FIPS
	Aruba Networks **AP-125**	N/A	6.1.4.0-FIPS
	Aruba Networks AP-134	N/A	6.1.4.0-FIPS
	Aruba Networks AP-135	N/A	6.1.4.0-FIPS
	Aruba Networks **AP-175P**	N/A	6.1.4.0-FIPS
	Aruba Networks AP-175AC	N/A	6.1.4.0-FIPS
	Aruba Networks AP-175DC	N/A	6.1.4.0-FIPS
	Aruba Networks **RAP-5WN**	N/A	6.1.4.0-FIPS

LEGEND:
AP   Access Point
FIPS   Federal Information Processing Standard
LDAP   Lightweight Directory Access Protocol
MMC   Multi-Service Mobility Controller
N/A   Not Applicable

PKI   Public Key Infrastructure
RADIUS Remote Access Dial In User Service
RAP   Remote Access Point
SysLog System Logger
UC   Unified Capabilities

10. TESTING LIMITATIONS.

a. End instruments and DoD secure communications devices were not available to support testing. Tests pertaining to those elements were not conducted. Representative measurements were recorded in place of actual test results. These measurements indicate a link quality that is both suitably high and represents a reasonably low risk affiliated with the use of these products.

b. Testing of traffic parameters used up to 50 independent flow streams. Current test equipment licensing constrains the number of flows to 50. This level of network traffic exceeds the typical amount representative for loading an AP used in a dedicated voice network. Constraining traffic flows to this quantity represents a low risk in properly assessing the SUT's capabilities against the "UCR 2008**,** Change 3."

11. INTEROPERABILITY EVALUATION RESULTS. The SUT meets the critical interoperability requirements for WLAS and WAB in accordance with (IAW) Section 5.3.1.7.2 of the "UCR 2008**,** Change 3*,"* and is certified for joint use with other ASLAN infrastructure products listed on the UC APL. Additional discussion regarding specific testing results is contained in subsequent sections.

11.1 Interfaces. The SUT's wireless interface statuses are provided in Table 2-5.

Table 2-5. Wireless Interface Requirements Statuses

Interface	Critical (See note 1.)	UCR Reference	Threshold CR/FR Requirements (See note 2.)	Status	Remarks
WLAS					
802.11a	N	5.3.1.7.2.3	1, 2, 3, 5, and 7	Certified	
802.11b	N	5.3.1.7.2.3	1, 2, 3, 5, and 7	Certified	
802.11g	N	5.3.1.7.2.3	1, 2, 3, 5, and 7	Certified	
802.16	N	5.3.1.7.2.3	1, 2, 3, 5, and 7	N/A	
802.3i	N	5.3.1.7.2.5	1, 2, 3, 5, and 7	Certified	
802.3j	N	5.3.1.7.2.5	1, 2, 3, 5, and 7	Certified	See note 3.
802.3u	N	5.3.1.7.2.5	1, 2, 3, 5, and 7	Certified	
802.3 z	N	5.3.1.7.2.5	1, 2, 3, 5, and 7	Certified	See note 3.
802.3ab	N	5.3.1.7.2.5	1, 2, 3, 5, and 7	Certified	
WAB					
802.11a	N	5.3.1.7.2.6	1, 2, 3, 6, and 7	Certified	
802.11b	N	5.3.1.7.2.6	1, 2, 3, 6, and 7	Certified	
802.11g	N	5.3.1.7.2.6	1, 2, 3, 6, and 7	Certified	
802.16	N	5.3.1.7.2.6	1, 2, 3, 6, and 7	N/A	
802.3i	N	5.3.1.7.2.6	1, 2, 3, 6, and 7	Certified	
802.3j	N	5.3.1.7.2.6	1, 2, 3, 6, and 7	Certified	See note 3.
802.3u	N	5.3.1.7.2.6	1, 2, 3, 6, and 7	Certified	
802.3z	N	5.3.1.7.2.6	1, 2, 3, 6, and 7	Certified	See note 3.
802.3ab	N	5.3.1.7.2.6	1, 2, 3, 6, and 7	Certified	
WEI					
802.11a	N	5.3.1.7.2.3	1, 3, and 4	N/A	Products tested did not include WEIs.
802.11b	N	5.3.1.7.2.3	1, 3, and 4	N/A	
802.11g	N	5.3.1.7.2.3	1, 3, and 4	N/A	
802.16	N	5.3.1.7.2.3	1, 3, and 4	N/A	

NOTES:
1. The "UCR 2008, Change 3," does not define any minimum interfaces. The SUT must minimally provide one of the wired interfaces (to the ASLAN) and wireless interfaces (subscriber).
2. The SUT need not provide wireless capabilities; however, if such capabilities are present, the SUT must meet all threshold CRs/FRs. The detailed CRs/FRs are listed in Enclosure 3, System Capability Requirements and Functional Requirements.
3. Support for this interface type is through the use of an appropriate SFP installed at the controller.

LEGEND:
ASLAN	Assured Services LAN	SUT	System Under Test
CR	Capability Requirement	UCR	Unified Capabilities Requirements
FR	Functional Requirement	WAB	Wireless Access Bridge
LAN	Local Area Network	WEI	Wireless End Instrument
N/A	Not Applicable	WLAS	Wireless LAN Access System
SFP	Small Form-Factor Pluggable		

11.2 Capability Requirements and Functional Requirements. The status of the SUT's CRs/FRs are listed in Table 2-6. The detailed CRs/FRs are provided in Table 3-1 of the System Capability Requirements and Functional Requirements.

Table 2-6. SUT Capability Requirements and Functional Requirements

CR/FR ID	Capability/Function	Applicability (See note 1.)	UCR Reference	Status	Remarks
	General Wireless Requirements				
	IPv6	Required	5.3.1.7.2.1	Met	See note 2.
	Wi-Fi Certified	Required (See note 3.)	5.3.1.7.2.1	Met	See note 4.
	Redundancy	Required	5.3.1.7.2.1	Met	
1	FIPS 140-2 Level 1	Required	5.3.1.7.2.1	Met	See note 4.
	Latency	Required	5.3.1.7.2.1	Met	
	Traffic Prioritization	Required	5.3.1.7.2.1	Met	
	Wireless STIGs	Required	5.3.1.7.2.1	Met	See note 5.
	CAPWAP	Required	5.3.1.7.2.1	Partially Met	TDR issued. See note 6
	WIDS				
2	Continuous Scanning			Met	See note 7.
	Location-sensing			Met	See note 7.
	Wireless Interface Requirements				
	Interface Standards	Required (See note 8.)	5.3.1.7.2.3	Met	
3	802.11 Interface Standards	Required (See note 9.)	5.3.1.7.2.3	Met	
	802.16 Interface Standards	Required (See note 10.)	5.3.1.7.2.3	N/A	See note 11.
	Fixed/Nomadic WEIs	Required (See note 12.)	5.3.1.7.2.3	N/A	See note 13.
	WEIs				
	VoIP Solution	Required (See note 14.)	5.3.1.7.2.4	N/A	
4	Access Methods	Required (See note 15.)	5.3.1.7.2.4	N/A	
	Call Control Authentication	Required (See note 14.)	5.3.1.7.2.4	N/A	
	Call Termination	Required (See note 12.)	5.3.1.7.2.4	N/A	
	WLAS Requirements				
	Loss of Call upon WLAS failure	Required (See note 16.)	5.3.1.7.2.5	Met	See note 17.
5	Maximum supported EIs	Required (See note 16.)	5.3.1.7.2.5	Met	See notes 17 and 18.
	MOS	Required (See note 16.)	5.3.1.7.2.5	Met	See notes 16 and 18.
	Roaming	Required (See note 16.)	5.3.1.7.2.5	Met	See note 17.
	WAB				
	Individual Interface Standards	Required (See note 9.)	5.3.1.7.2.6	Met	For specified interfaces.
	Maximum Voice Calls Transported	Required (See note 9.)	5.3.1.7.2.6	Met	See notes 17 and 18.
	Voice MOS	Required (See note 9.)	5.3.1.7.2.6	Met	See note 17.
6	E2E BER	Required (See note 9.)	5.3.1.7.2.6	Met	
	Secure Voice Transmission	Required (See note 9.)	5.3.1.7.2.6	Met	See note 19.
	Call Signaling Transport	Required (See note 9.)	5.3.1.7.2.6	Met	See note 19.

Table 2-6. SUT Capability Requirements and Functional Requirements (continued)

	Latency	Required (See note 9.)	5.3.1.7.2.6	Met	
	Jitter	Required (See note 9.)	5.3.1.7.2.6	Met	TDR issued. See note 20.
	WLAS/WAB Combination	Required (See note 9.)	5.3.1.7.2.6	Met	
7	**ASLAN Requirements Applicable to Wireless Products**				
	General Performance Parameters	Required	5.3.1.3	Met	

NOTES:
1. The SUT need not provide wireless capability. However, if wireless capability is present, the SUT must meet the wireless requirements (as applicable for product type WLAS, WAB, or WEI) in order to be certified.
2. Vendor demonstrated IPv6 management and packet transfer via wireless and wired Ethernet.
3. Only applies to 802.11 interfaces.
4. Verified via vendor LoC and testing.
5. Vendor met STIG requirements with submitted mitigations.
6. The TDR was adjudicated by DISA on 10 July 2012, and was determined to be "Conditions of Fielding" with operations limited to using Aruba Wireless Controllers.
7. The SUT support WIDS extensive features of continuous scanning and location sensing.
8. Individual sub-requirements apply to specific interface types.
9. Applicable to 802.11 interfaces only.
10. Applicable to 802.16 interfaces only.
11. SUT does not provide 802.16 interface.
12. Applies to WEIs; not applicable to WLASs or WABs.
13. SUT does not include WEIs.
14. The WEI is certified in conjunction with a call-control agent (VoIP solution).
15. The WEI may be dedicated service (single traffic type) or shared service (voice, video, and data).
16. Specified requirements are only applicable to WLAS products.
17. Verified via emulated VoIP phone calls using test, measurement and diagnostic equipment.
18. The SUT was not tested to the maximum 96 EIs – see Testing Limitations (Section 10).
19. No direct measurement available. Reference the SUT's demonstrated suitable quality wireless transport confirmed with collaborating measurements. The SUT is considered to meet this requirement with a low-risk assessment.
20. The TDR was adjudicated by DISA on 10 July 2012, and was determined to be "Change Requirement" from 1ms, allowing for 3 ms or less jitter.

LEGEND:

802.11	IEEE Set of Wireless Standards in the 2.4,3.6, and 5 GHz	LoC	Letter of Compliance
		MOS	Mean Opinion Score
802.16	IEEE Series of Wireless Broadband Standards	ms	Millisecond
ASLAN	Assured Services LAN	N/A	Not Applicable
BER	Bit Error Rate	STIG	Security Technical Implementation Guide
CAPWAP	Control and Provisioning of Wireless Access Point	SUT	System Under Test
CR	Capability Requirement	TDR	Test Discrepancy Report
DISA	Defense Information Systems Agency	UCR	Unified Capabilities Requirements
E2E	End-to-End	WAB	Wireless Access Bridge
EIs	End Instruments	WEI	Wireless End Instrument
FIPS	Federal Information Processing Standard	WIDS	Wireless Intrusion Detection System
FR	Functional Requirement	Wi-Fi	Trademark of the Wi-Fi Alliance that Refers to a Range of Connectivity Technologies Including WLAN
GHz	Gigahertz		
IEEE	Institute of Electrical and Electronics Engineers	WLAN	Wireless LAN
ID	Identification	WLAS	Wireless LAN Access System
IPv6	Internet Protocol Version 6	VoIP	Voice Over Internet Protocol
LAN	Local Area Network		

a. **General Wireless Requirements**.

(1) Internet Protocol Version 6 (IPv6). The SUT WLAS (Figure 2-2) test configuration was used to investigate support for this requirement. The SUT wireless controllers support SSL web management using both Internet Protocol Version 6 (IPv4) and IPv6 addressing. Testing confirms IPv6 packets are allowed to traverse the SUT in both WLAS and WAB configurations without issue. Tests were conducted using wired and wireless clients connected at various locations to confirming Layer 2 (L2) transport of the IPv6 packets. The SUT's wireless domain operates at an Open System Interconnection (OSI) L2 level. Thus all properly formatted Ethernet frames may traverse the system. The SUT meets this requirement.

(2) Wi-Fi Alliance Certifications, WPA2-Enterprise, and Wi-Fi Multimedia (WMM). The SUT has Wi-Fi Alliance Certifications for Enterprise WPA2 and WMM published on record at Wi-Fi Alliance's publicly accessible website at http://www.wi-fi.org. The SUT meets this requirement.

(3) Wireless support for immediate/priority (I/P), required (R), and non-mission critical users. The SUT provides suitable wireless support for I/P, R, and non-mission critical users. The SUT provides an L2 wireless transport. All properly crafted Ethernet frames may be transported transparently across the SUT. This was confirmed using network traffic generation in conjunction with network traffic analysis. The SUT supports this requirement.

(4) Redundancy. The WLAS (Figure 2-2) test configuration was used to confirm this requirement. All the SUT wireless controllers support failover between primary and subordinate controllers. Tests confirmed each wireless controller listed was involved in a failed state and was the responsible recovery unit. The Aruba 6000 series controllers meet the Single Product Redundancy requirements. This model supports the capabilities for multiple processors and power supplies. All the SUT wireless controllers meet the Dual Product Redundancy requirements. Wireless controller transition times were measured at a range of 26 to 32 seconds for network restoration. All the SUTs wireless controllers support Virtual Router Redundancy Protocol (VRRP) for synchronization and coordination of alternate controllers. This satisfies the Redundancy Protocol requirement for Dual Product Redundancy UC 5.3.1.7.2.1-4b. Tests confirmed all the SUT APs listed support failover and recovery. Wireless clients successfully migrated to alternate APs without intervention.   The AP failovers were rapid and consistent. Tests confirmed successful client transition to alternate APs assessment by observing a brief 0.6- to 5-second service interruption. The SUT meets this requirement.

(5) FIPS 140-2. All the SUT wireless controllers are FIPS 140-2 certified. There are certifications published on the National Institute of Standards and Technology (NIST) website. The SUT meets this requirement.

(6) Wireless LAN Bridging Delay. The SUTs use of wireless via an AP does not increase LAN latency by more than 10 milliseconds (ms). Testing confirms the SUT's APs one-way delay averaged 6 ms. The SUT meets this requirement.

(7) Support for LAN Prioritization and Quality of Service (QoS). The SUT supports IEEE 802.11 interfaces. These interfaces support IEEE 802.11e implementing Differentiated Services Code Point (DSCP) and published WMM certification. The SUT also supports WMM Power Save. Also, confirmed by publication on Wi-Fi.org. The SUT meets this requirement.

(8) Wireless Security Technical Implementation Guide (STIG) Compliance. The SUT has published WPA2-Enterprise Certification on record. It supports AES-Counter-Mode/Cipher Block Chaining [CBC] Message Authentication Code [MAC] Protocol (CCMP), and Extensible Authentication Protocol – Transport Layer Security (EAP-TLS) IAW IEEE 802.11i. The SUT meets this requirement.

(9) Wireless Systems Meet Access Requirements. The SUT meets all previously stated requirements for access products.

(10) Control and Provisioning of Wireless Access Points (CAPWAPs). The SUT does not support CAPWAP. Use of CAPWAP limits the management scope and security posture of the SUT and affiliated APs. The SUT provides comprehensive enterprise level security and management capabilities for wired and wireless resources. The SUT met this requirement after Defense Information Systems   Agency (DISA) adjudication of Test Discrepancy Report (TDR) on 10 July 2012, with a "Condition of Fielding" that the SUT be deployed only with Aruba wireless controllers pending additional research on this requirement.

b. Wireless Intrusion Detection System (WIDS).

WIDS testing is not specified in the Joint Interoperability Test Command (JITC) UC Wireless IO Test Plan. WIDS is supported in the SUT.

(1) Continuous Scanning. The SUT supports continuous scanning WIDS capabilities. These capabilities were confirmed for all APs. The SUT can manage RF security, including user location and mapping, real-time monitoring, proactive alerts, historical reporting, and provide troubleshooting forensics. The SUT meets this requirement.

(2) Location-Sensing. The SUT supports location sensing WIDS capabilities. When deployment maps are integrated with Global Positioning System (GPS) coordinates the SUT provides comprehensive tracking of RF signals. The SUT meets this requirement.

c. Wireless Interface Requirements.

(1) WLAS interface support. The SUT supports the following:

- 802.11a IAW 802.11-2007 – 5 GHz
- 802.11b IAW 802.11-2007 – 2.4 GHz
- 802.11g IAW 802.11-2007 – 2.4 GHz
- 802.11n-2009 – 2.4 GHz and 5 Ghz

The SUT meets this requirement.

(2) SUT support for IEEE 802.11e and IEEE 802.11i The SUT supports IEEE 802.11e and IEEE 802.11i. These were confirmed during the IA and IO testing. The SUT meets this requirement.

(3) SUT support for IEEE 802.11a interfaces with IEEE 802.11h. The SUT APs all support IEEE 802.11a interface operations with IEEE 802.11h as an option which may be enabled through the management console. The SUT meets this requirement.

d. WEI Requirements.

The SUT is not a WEI, so all WEI requirements are not applicable.

e. WLAS Requirements.

(1) Failure of WLAS. The SUT AP failovers were rapid and consistent. Tests confirmed successful client transition to alternate APs assessment by observing a brief 0.6- to 5-second service interruption. The SUT meets this requirement.

(2) WLAS maximum EIs.   Testing of Voice over Internet Protocol (VoIP) flows was constrained to 50 due to licensing limitations. The WLAS measurements of the SUT APs ranged from Mean Opinion Score (MOS) 3.7 to 4.3 when using the 50 VoIP flows in association with loading traffic. These MOS values meet the Strategic-to-Tactical requirement of MOS 3.6 or better. Reference the "UCR 2008, Change 3," Table 5.3.1-8, Maximum Number of EIs Allowed per WLAS, a link speed of 10 Megabits per second (Mbps) is representative of a WiFi WLAS link speed, supporting a maximum of 96 wireless phone subscribers. Testing confirms the SUT is capable of supporting 50 wireless phone subscribers at the Strategic-to-Tactical level or better. It is reasonable to conclude, at a minimum level of risk, the SUT is capable of supporting the maximum number of wireless phone subscribers at this level of quality. The SUT meets this requirement.

(3) WLAS MOS. Determine the maximum number of VoIP subscribers where MOS degrades to a specified level. Testing of VoIP flows was constrained to 50 due to licensing limitations. The WLAS measurements of the SUT APs ranged from

MOS 3.7 to 4.3 when using the 50 VoIP flows in association with loading traffic. These MOS values meet the Strategic-to-Tactical requirement of MOS 3.6 or better. The SUT meets this requirement.

(4) WLAS Roaming. The WLAS transmitters shall not drop an active call as WEIs roam from one WLAS transmitter to another. Test measurements using network call emulation of wireless clients in association with each of the SUT APs confirm the successful migration between APs while maintaining network VoIP calls. The SUT meets this requirement.

(5) WLAS Trunk Interfaces. The SUT APs support the following interfaces:

- 10 Mbps IAW IEEE 802.3i
- 10 Mbps IAW IEEE 802.3j (requires appropriate SFP used at the controller)
- 100 Mbps IAW IEEE 802.3u
- 1000 Mbps IAW IEEE 802.3z (requires appropriate SFP used at the controller)
- 1000 Mbps IAW IEEE 802.3ab

The SUT and APs meet this requirement.

f. Wireless Access Bridge Requirements.

(1) WAB Wireless Interfaces. The SUT APs support the following interfaces:

- 10 Mbps IAW IEEE 802.3i
- 10 Mbps IAW IEEE 802.3j (requires appropriate SFP used at the controller)
- 100 Mbps IAW IEEE 802.3u
- 1000 Mbps IAW IEEE 802.3z (requires appropriate SFP used at the controller)
- 1000 Mbps IAW IEEE 802.3ab

Additionally, the SUT WABs supports IEEE 802.11 a/b/g/n IAW 802.11 QoS specified in UC 5.3.1.7.2.1. The SUT meets this requirement.

(2) WAB's maximum number of voice calls transported. Reference the "UCR 2008, Change 3," Table 5.3.1-9, LAN VoIP Subscribers for IPv4 and IPv6. The table shows a Distribution IP trunk link pair at 10 Mbps, supporting 25 Mission Critical VoIP subscribers, or 50 Non-Mission Critical VoIP subscribers. The 10 Mbps link is representative of the wireless capacity. Testing of VoIP flows was constrained to 50 due to licensing limitations. The WLAS/WAB configuration measurements of the SUT APs ranged from MOS 3.6 to 4.3 when using the 50 VoIP flows in association with loading traffic. These MOS values meet the Strategic-to-Tactical requirement of MOS 3.6 or better. The SUT meets this requirement.

(3) WAB MOS measurements. The introduction of a WAB(s) shall not cause the End-to-End (E2E) average MOS to fall below appropriate levels (Strategic 4.0, Strategic-to-Tactical 3.6, and Tactical-to-Tactical 3.2) as measured over any 5-minute time interval. Testing of VoIP flows was constrained to 50 due to licensing limitations. The WLAS/WAB configuration measurements of the SUT APs ranged from MOS 3.6 to 4.3 when using the 50 VoIP flows in association with loading traffic. These MOS values meet the Strategic-to-Tactical requirement of MOS 3.6 or better. The SUT meets this requirement.

(4) WAB Bit Error Rate (BER). The introduction of a WAB(s) shall not exceed the E2E digital BER requirement of less than one error in 1x10-8 (averaged over a 9-hour period). The 9-hour test period was adapted to 1 hour to accommodate for the higher throughput of contemporary WABs. This adjustment was coordinated with JITC on 3 April 2012. Reference "UCR 2008, Change 3," Section 5.3.1.3-4a, Packet Loss for Voice Packets. Packet loss measured within the configured queuing parameters shall be measured to no more than 0.015 percent for Access, Distribution, and Core products. Packet loss measurements recorded for the SUT in WLAS/WAB configuration ranged from 0.004 to 0.442 percent. Over half the measurements recorded meet the "UCR 2008, Change 3," Section 5.3.1.3.-4a, Packet Loss for Voice Packets, requirement of no more than 0.015 percent. There exists plausible uncontrolled external RF influences that may result in varying magnitudes of packet loss. Given the recorded measurements meeting the requirement, the SUT has successfully demonstrated an ability to meet the requirements. The recorded values in excess of the requirement can be attributed variability due to uncontrolled external RF influences. Multiple measurements taken using stable configurations demonstrated large magnitude variability in packet loss. Additional testing minimized equipment bias as a significant factor contributing to excess packet loss. The SUT meets this requirement.

(5) WAB DoD Secure Communications Device (DSCD) Operations. The introduction of a WAB(s) shall not degrade secure transmission for secure end products, as defined in the UCR 2008 Change 3, Section 5.2.12.6, DoD Secure Communications Devices (DSCDs). The DSCDs were not tested. They were not available to support testing. The SUT WAB demonstrated the ability to provide quality L2 wireless data transport on the basis of satisfying UC requirements for proper traffic management, traffic transparency, speed, latency, and packet loss. Thus, the SUT has confirmed a low-risk assessment for supporting DSCD operations. The SUT meets this requirement.

(6) WAB Transparency. The WAB shall transport all call control signals transparently on an E2E basis. The SUT WAB provides an L2 wireless transport. All properly crafted Ethernet frames may be transported transparently across the WAB. This was confirmed using network traffic generation in conjunction with network traffic analysis. The SUT meets this requirement.

(7)   WAB Delay. The addition of a WAB(s) shall not cause the one-way delay measured from ingress to egress to increase by more than 3 ms for each WAB used, averaged over a 5-minute period. Reference the "UCR 2008, Change 3," Section 5.3.1.3-2a, Voice/Signaling Packets. No more than 2 ms latency. The aggregation of both requirements establishes the requirement for WAB delay at no more than 5 ms. The SUT WAB delay results ranged from 3 ms to 6 ms with only one measurement meeting the < 6 ms requirement. Remaining measurements were 6 ms delay. The SUT demonstrated successful achievement of the requirement on one test case. The majority of the measurements exceed the requirement by 1 ms. Reference the plausibility of external influence as stated in the WAB BER and observed throughout the test activity. The affiliated MOS measurements meet the required values with these 6 ms delay values. There is a low-risk assessment with the SUT in meeting this requirement. The SUT meets this requirement.

(8)   WAB Jitter. The addition of the WAB shall not increase the LAN jitter requirements previously specified in this section. All Core, Distribution, and Access products shall have the capability to transport prioritized packets (media and signaling) as follows. The jitter shall be achievable over any 5-minute period measured from ingress ports to egress ports under congested conditions. A congested condition is defined as 100 percent bandwidth utilization. Voice Packets. No more than 1 ms jitter. The SUT WAB jitter results ranged from 1.032 ms to 2.336 ms. These values exceed the requirement by 0.032 ms to 1.336 ms. Reference the plausibility of external influence as stated in the WAB BER and observed throughout the test activity. The affiliated MOS measurements meet the required values with the jitter measurements in excess of this requirement. There is a low-risk assessment associated with the SUT's jitter values. The SUT meets this requirement after DISA TDR adjudication on 10 July 2012, issuing a "Change Requirement" to permit 3 ms or less for WAB jitter.

(9)   WLAS/WAB Simultaneous Operations, Service Class Tagging/QoS. The WAB(s) and/or WLAS/WAB shall support Service Class tagging/QoS as previously specified in this section. Reference "UCR 2008, Change 3," Section 5.3.1.7.2.1-7a: Wireless products using IEEE 802.11 shall use the settable Service Class Tagging/QoS parameters within 802.11e to implement, as a minimum, DSCP. The product shall support WMM. Wireless mobile devices shall also support WMM Power Save. The SUT demonstrated the ability to manage traffic based on Service Class Tagging/QoS/DSCP. The SUT is certified to support WMM and WMM Power Save. This is confirmed with the certificate for record posted on Wi-Fi Alliance's publically accessible website at http://www.wi-fi.org. The SUT meets this requirement.

(10) WAB call support. The WABs may support Flash Override/Flash (FO/F) calls, I/P, R, and non-mission critical calls. All calls must meet other specified performance requirements for non-mission critical users. Reference "UCR 2008, Change 3," Section 5.3.1.7.2.1-3: Wireless networks may support I/P, R, and non-mission critical users, but shall not be used to support FO/F users. The SUT provides an L2 wireless transport. All properly crafted Ethernet frames may be transported

transparently across the SUT. This was confirmed using network traffic generation in conjunction with network traffic analysis. The SUT supports this requirement.

11.3 Information Assurance. The IA Assessment Report is published separately and is provided under a separate cover.

12. TEST AND ANALYSIS REPORT. In accordance with the Program Manager's request, no detailed test report was developed. The JITC distributes interoperability information via the JITC Electronic Report Distribution (ERD) system, which uses Unclassified But Sensitive Internet Protocol Router Network (NIPRNet) e-mail. More comprehensive interoperability status information is available via the JITC System 2-7 Tracking Program (STP). The STP is accessible by .mil/gov users on the NIPRNet at https://stp.fhu.disa.mil. Test reports, lessons learned, and related testing documents and references are on the JITC Joint Interoperability Tool (JIT) at http://jit.fhu.disa.mil (NIPRNet). Information related to DSN testing is on the Telecom Switched Services Interoperability (TSSI) website at http://jitc.fhu.disa.mil/tssi.

SYSTEM FUNCTIONAL AND CAPABILITY REQUIREMENTS

The required and conditional features and capabilities for wireless products are established by Section 5.3.1.7.2 of the "Department of Defense Unified Capabilities Requirements 2008 (UCR 2008), Change 3." The SUT need not provide conditional features and capabilities; however, if they are present, they must function according to the specified requirements. The detailed Functional Requirements (FRs) and Capability Requirements (CRs) for wireless products are listed in Table 3-1.

Table 3-1. Wireless Products Capability/Functional Requirements

ID	Requirement	Reference	IO	IA	Remarks
		Wireless Requirements			
1	Meet the IP requirements detailed in the DISA UCR 2008 IPv6 Requirements.	UCR 2008: 5.3.1.7.2.1 (1)	X		All TP IO-1 (see IDs 363-491)
2	802.11 wireless products must be WiFi Alliance Certified.	UCR 2008: 5.3.1.7.2.1 (2)		X	All TP IA-1
3	Wireless networks shall not be used to support special C2 users.	UCR 2008: 5.3.1.7.2.1 (3)	X		All TP IO-2
4	For wireless products that provide transport to more than 96 telephony users, the wireless products shall provide redundancy (single or dual).	UCR 2008: 5.3.1.7.2.1 (4)	X		WLAS/WAB TP IO-3
5	FIPS 140-2 Level 1/2	UCR 2008: 5.3.1.7.2.1 (5)		X	All Level 1 – secure room; Level 2 open area (See ID 236-Table E-9 Test Case 342.)
6	The use of wireless in the LAN shall not increase latency by more than 10 ms above the specified maximum latency for a wired LAN.	UCR 2008: 5.3.1.7.2.1 (6)	X		All TP IO-4
7	Support LAN Traffic Prioritization: 802.11: 802.11e DSCP 802.16: 80216d and/or 802.16e	UCR 2008: 5.3.1.7.2.1 (7)	X		All TP IO-5
8	Wireless products shall meet the WLAN security requirements as stipulated in the Wireless STIG, and all 802.11 components shall: Use AES-CCMP using 802.11i Implement EAP-TLS	UCR 2008: 5.3.1.7.2.1 (8)		X	WLAS/WEI This requirement does not apply to connections between 802.11 WABs. TP IA-2
9	The WLAS and/or WAB wireless network shall be monitored by a Wireless Intrusion Detection System (WIDS) device under test.	UCR 2008: 5.3.1.7.2.2		X	WLAS/WAB TP IA-3
10	Wireless Interface Requirements: All 802.11: support 802.11e – Part 11and Amendments 6 and 8 802.11a: 802.11h Part 11 and Amendment 5 802.16 (fixed): 802.16d or 802.16e and Amendment 2 802.16 (nomadic): 802.16e and Amendment 2	UCR 2008: 5.3.1.7.2.3	X		All TP IO-6

Table 3-1. Wireless Products Capability/Functional Requirements Table (continued)

ID	Requirement	Reference	IO	IA	Remarks
		Wireless Requirements			
11	WEIs shall: - Use 802.11 or 802.16 - Support dedicated or shared access method - Support authentication IAW IA - Provide telephone functionality identical to VoIP wired phone - Minimum FIPS 140-2 level 1 -VoIP timeout 0-60sec ; 5 sec default (VoIP device under test requirement)	UCR 2008: 5.3.1.7.2.4	X	X	WEI TP IO-7 For FIPs, see ID 236-Table E-9 Test Case 342.
12	WLAS must support: - No loss of calls for primary failover to secondary WLAS - support max EIs as defined by MOS when all telephones are off hook simultaneously (table 5.3.1-9) -not drop active call when WEI roams from one WLAS to another.	UCR 2008: 5.3.1.7.2.5	X		WLAS/WEI Maximum Number of EIs Allowed per WLAS, for converged or non-converged access for redundant and non-redundant WLAS; while not degrading any of the individual EIs' voice quality below the specified MOS scores for strategic and tactical situations, in an open-air environment at a distance of 100 feet, except for the 5-second re-authentication as stated in item 1, (i.e., strategic MOS 4.0, strategic-to-tactical MOS 3.6, tactical-to- tactical MOS 3.2). TP IO-8
13	If WABs support 802.16 it must support 802.16d Part 16 or 802.16e part 16 and Amendment 2	UCR 2008: 5.3.1.7.2.6 (1)	X		WAB TP IO-9
14	Max WAB voice calls IAW 5.3.1.7.3 Traffic engineering	UCR 2008: 5.3.1.7.2.6 (2)	X		WAB TP IO-10
15	The introduction of a WAB(s) shall not cause the end-to-end average MOS to fall below appropriate levels (strategic 4.0, strategic-to-tactical 3.6, and tactical-to-tactical 3.2)	UCR 2008: 5.3.1.7.2.6 (3)	X		WAB As measured over any 5-minute time interval. TP IO-11
16	The introduction of a WAB(s) shall not exceed the end-to-end digital BER requirement of less than 1 error in 1×10^{-8} (averaged over a 9-hour period).	UCR 2008: 5.3.1.7.2.6 (4)	X		WAB TP IO-12
17	The introduction of a WAB(s) shall not degrade secure transmission for secure end products as defined in UCR 2008, Section 5.2.12.6, DOD Secure Communications Devices (DSCDs).	UCR 2008: 5.3.1.7.2.6 (5)	X		WAB TP IO-13
18	The WAB shall transport all call control signals transparently on an end-to-end basis	UCR 2008: 5.3.1.7.2.6 (6)	X		WAB TP IO-14
19	The addition of a WAB(s) shall not cause the one-way delay measured from ingress to egress to increase by more than 3 ms for each WAB used, averaged over any 5-minute period.	UCR 2008: 5.3.1.7.2.6 (7)	X		WAB TP IO-15
20	The addition of the WAB shall not increase the LAN jitter requirements previously specified in this section	UCR 2008: 5.3.1.7.2.6 (8)	X		WAB TP IO-16

Table 3-1. Wireless Products Capability/Functional Requirements Table (continued)

ID	Requirement	Reference	IO	IA	Remarks
ASLAN Requirements Applicable to Wireless Components
21	WLAS/WAB combination shall: - support Service Class tagging/QoS. - WAB may support special C2 calls, C2, C2(R), and non-C2 calls. All calls must meet other specified performance requirements for these users.	UCR 2008: 5.3.1.7.2.6	X		WLAS/WAB TP IO-17
ASLAN Requirements Applicable to Wireless Components
22	All ASLAN C/D/A components must be non-blocking for a minimum of 50% rated output capacity.	UCR 2008: 5.3.1.3 (1)	X		WLAS/WAB TP IO-18
23	All ASLAN C/D/A components shall transport prioritized voice with no more than 2 ms latency.	UCR 2008: 5.3.1.3 (2)	X		WLAS/WAB Xref: IDs 6 and 19 (TPs IO-4 and IO-15)
24	All ASLAN C/D/A components shall transport prioritized voice with no more than 1 ms jitter.	UCR 2008: 5.3.1.3 (3)	X		WLAS/WAB Achievable over any 5-minute period measured from ingress ports to egress ports under congested conditions. XRef: ID 20 (TP IO-16)
25	All ASLAN C/D/A components shall transport prioritized voice with no more than 0.02 % (C/D) and 0.01%(A) packet loss.	UCR 2008: 5.3.1.3 (4)	X		WLAS/WAB Achievable over any 5-minute period measured from ingress ports to egress ports under congested conditions. TP IO-19
26	All ASLAN C/D/A components shall transport prioritized voice with no more than a BER of 1 bit error in 10^6 bits.	UCR 2008: 5.3.1.3 (5)	X		WLAS/WAB Achievable over any 5-minute period measured from ingress ports to egress ports under congested conditions TP IO-20
27	This test will demonstrate whether the device under test can receive alarms, policy violations, and performance issues.	UCR 2008: 5.3.1.6.4 & 5.3.2.17.3.1.5	X		WLAS/WAB TP IO-21
VoIP Device under Test Requirements Applicable to Wireless Components
28	Supports VoIP device under test Codec for WEIs (G.711 with 20 ms).	UCR 2008: 5.2.12.8.2.2	X		WEI TP IO-22
29	Supports VoIP MLPP.	UCR 2008: 5.2.12.8.2.3	X		WEI TP IO-23
30	VoIP Device under test latency 60 ms (+ 10 ms for wireless).	UCR 2008: 5.2.12.8.2.7	X		All XRef: ID 6. Averaged over any 5-minute period. The latency is to be measured from IP handset to egress from the VoIP device under test via a DSN trunk. TP IO-24
IA Requirements Applicable to Wireless Components (**"Test case"** refers to the RTS IATP test case.)
31	The device under test shall be capable of being configured in accordance with all applicable DOD-approved security configuration guidelines (i.e., STIGs).	UCR 2008: 5.4.6.2 (1)		X	WLAS/WAB Table E-7, Test Case 1

Table 3-1. Wireless Products Capability/Functional Requirements Table (continued)

ID	Requirement	Reference	IO	IA	Remarks
IA Requirements Applicable to Wireless Components **("Test case" refers to the RTS IATP test case.)**
32	Software patches shall only be installed if they originate from the device under test manufacturer and are applied in accordance with manufacturer's guidance. The device under test shall only accept automatic software updates if the software vendor cryptographically signs them.	UCR 2008: 5.4.6.2. (1.c and 1.c.1)		X	All Table E-7, Test Case 4 and 5
33	If the device under test uses public domain software, unsupported software, or other software, it shall be covered under that device under test's warranty.	UCR 2008: 5.4.6.2 (2) (Conditional)		X	All Table E-7, Test Case 6
34	The device under test shall only use open source software if all licensing requirements are met.	UCR 2008: 5.4.6.2 (2.a)		X	All Table E-7, Test Case 7
35	The device under test shall not use mobile code technologies (e.g., Java, JavaScript, VBScript, and ActiveX) unless the mobile code technology is categorized and controlled in accordance with policy.	UCR 2008: 5.4.6.2 (3)		X	All Table E-7, Test Case 8
36	If Softphones are used in remote connectivity situations, the device under test shall be capable of supporting a VPN for VVoIP traffic from the PC to Enclave VPN access router/node. Note: The data from the PC and VVoIP traffic from the PC Softphone must be separated into the appropriate VLANs at the earliest point in the path.	UCR 2008: 5.4.6.2 (4)		X	Conditional WEI Table E-7, Test Case 9
37	The device under test shall be capable of being located in physically secure areas.	UCR 2008: 5.4.6.2 (5)		X	WLAS/WAB Table E-7, Test Case 10
38	If the device under test has a speakerphone, the device under test shall be capable of disabling the speakerphone microphone. Note: Acceptable methods to meet this requirement include physically disabling the speakerphone or disabling the speakerphone using a configurable software parameter.	UCR 2008: 5.4.6.2 (6)		X	Conditional WEI Table E-7, Test Case 13
39	If the device under test is used in a sensitive area where National Security devices under test (NSS) are employed and/or within environments where National Security Information (NSI) is stored, processed, or transmitted, then the device under test shall be certified and accredited in accordance with the TSG 6, which is prepared by the NTSWG.	UCR 2008: 5.4.6.2 (7)		X	Conditional WEI Table E-7, Test Case 14
40	The device under test shall be capable of using a static IP address.	UCR 2008: 5.4.6.2 (8)	X	X	All Table E-7, Test Case 15 TP IO-25

Table 3-1. Wireless Products Capability/Functional Requirements Table (continued)

ID	Requirement	Reference	IO	IA	Remarks
IA Requirements Applicable to Wireless Components ("Test case" refers to the RTS IATP test case.)
41	If the device under test uses a Microsoft Windows based operating system, the device under test shall support the installation and operation of the DOD-mandated Host Based Security Device under test (HBSS).	UCR 2008: 5.4.6.2 (10)		X	Conditional WEI Table E-7, Test Case 17
42	The device under test shall be capable of displaying the latest DOD warning banners on all system management ingress ports accessed by administrators or users as part of a human-to-machine interface.	UCR 2008: 5.4.6.2.1.1 (1)		X	WLAS/WAB Table E-8, Test Case 18
43	At the first point of entry, the device under test shall have the capability to display a warning message of up to 20 lines by 80 characters (1600 characters) in length. As part of delivered software, the device under test shall be capable of providing an appropriate default message that warns against unauthorized access or use. The device under test banner shall be capable of being configured by authenticated and authorized personnel. The device under test shall be capable of displaying the banner to the administrator or user prior to a login attempt to the device under test	UCR 2008: 5.4.6.2.1.1 (1.a -1.d)		X	WLAS/WAB Table E-8, Test Cases 18-22
44	The device under test shall be capable of displaying the following information upon successful access: device under test shall be capable of displaying the date and time of the administrator's or user's last successful access to the device.	UCR 2008: 5.4.6.2.1.1 (1.f) UCR 2008: 5.4.6.2.1.1 (1.f.1)		X	WLAS/WAB Table E-8, Test Cases 25-26
45	The device under test shall be capable of displaying the number of unsuccessful attempts by that user-ID to gain access to the device under test (e.g., mistyped password) since the last successful access by that user-ID.	UCR 2008: 5.4.6.2.1.1 (1.f.2)		X	WLAS/WAB Table E-8, Test Case 27
46	The device under test shall be identified by an entity identifier that is unique within the domain of the appliance or application being connected to.	UCR 2008: 5.4.6.2.1.2 (1)		X	All Table E-8, Test Case 28
47	The device under test shall be capable of providing a primary access control method that is stronger than assigning passwords to specific actions (e.g., operations-related commands), although assigning passwords may be used to augment access control.	UCR 2008: 5.4.6.2.1.2 (1.a)		X	All Table E-8, Test Case 29
48	The device under test shall be capable of ensuring that all users and customer passwords are used in a secure manner.	UCR 2008: 5.4.6.2.1.2 (1.b)		X	WLAS/WAB Table E-8, Test Case 30
49	The device under test shall be capable of automatically suppressing or blotting out the clear text representation of a password on the data entry device.	UCR 2008: 5.4.6.2.1.2 (1.b.1)		X	All Table E-8, Test Case 31

Table 3-1. Wireless Products Capability/Functional Requirements Table (continued)

ID	Requirement	Reference	IO	IA	Remarks
IA Requirements Applicable to Wireless Components ("Test case" refers to the RTS IATP test case.)					
50	The device under test shall ensure that passwords are safeguarded at the confidential level for sensitive but unclassified (SBU) devices under test.	UCR 2008: 5.4.6.2.1.2 (1.b.2)		X	All Table E-8, Test Case 32
51	The device under test shall be capable of storing access passwords (user and administrator) in a one-way encrypted form.	UCR 2008: 5.4.6.2.1.2 (1.b.2.a)		X	All Table E-8, Test Case 33
52	The device under test shall be capable of ensuring that passwords are not available in clear text to any user, including appropriate administrators. An appropriate administrator may be allowed to retrieve encrypted passwords. However, encrypted passwords shall not be available to any other user.	UCR 2008: 5.4.6.2.1.2 (1.b.3)		X	All Table E-8, Test Case 34
53	The device under test shall be capable of providing a mechanism for a password to be user changeable. This mechanism shall require re-authentication of user identity.	UCR 2008: 5.4.6.2.1.2 (1.b.4)		X	All Table E-8, Test Case 35
54	The device under test shall be capable of ensuring that a new user password differs from the previous password by at least four characters.	UCR 2008: 5.4.6.2.1.2 (1.b.4.a)		X	All Table E-8, Test Case 36
55	The device under test shall be capable of having a password history to prevent password reuse. The default shall be configurable and shall be at least the past eight passwords or 180 days of password history.	UCR 2008: 5.4.6.2.1.2 (1.b.4.b)		X	All Table E-8, Test Case 37
56	After a password is assigned to a human user, when that user establishes a session for the first time, the device under test shall be capable of prompting the user to change the password and deny the session if the user does not comply.	UCR 2008: 5.4.6.2.1.2 (1.b.5)		X	WLAS/WAB Table E-8, Test Case 38
57	The device under test shall be capable of enforcing a configurable password aging interval (i.e., a password is required to be changed after a specified interval).	UCR 2008: 5.4.6.2.1.2 (1.b.6)		X	WLAS/WAB Table E-8, Test Case 39
58	The device under test shall be capable of defining a device under test-wide default password aging interval.	UCR 2008: 5.4.6.2.1.2 (1.b.6.a)		X	WLAS/WAB Table E-8, Test Case 40
59	If the device under test supports long-lived sessions (i.e., two signaling appliances continuously connected), the device under test shall be capable of providing the capability to set the password ageing interval on a "per-user-ID-basis	UCR 2008: 5.4.6.2.1.2 (1.b.6.b)		X	WLAS/WAB Table E-8, Test Case 41
60	The device under test shall be capable of setting the password aging interval on a "per-user-ID basis.	UCR 2008: 5.4.6.2.1.2 (1.b.6.c)		X	WLAS/WAB Table E-8, Test Case 42
61	The device under test shall notify the user a specified period of time before the password expiration.	UCR 2008: 5.4.6.2.1.2 (1.b.6.c.i)		X	WLAS/WAB Table E-8, Test Case 42

Table 3-1. Wireless Products Capability/Functional Requirements Table (continued)

ID	Requirement	Reference	IO	IA	Remarks
IA Requirements Applicable to Wireless Components ("Test case" refers to the RTS IATP test case.)				
62	The device under test shall notify the user upon password expiration, but allow a specified additional number of subsequent logins within a specified time period before requiring a new password. The default for the number of subsequent logins shall not be greater than three. The default for the specified time period shall not be greater than 30 days.	UCR 2008: 5.4.6.2.1.2 (1.b.6.c.ii)		X	WLAS/WAB Table E-8, Test Case 42
63	The device under test shall not hard code the notification mechanism for password expiration to allow for variation in variables such as "early warning period," "grace period," and subsequent login after password expiration.	UCR 2008: 5.4.6.2.1.2 (1.b.6.c.iii)		X	WLAS/WAB Table E-8, Test Case 42
64	The device under test shall notify the user a specified period of time before the password expiration.	UCR 2008: 5.4.6.2.1.2 (1.b.6.d)		X	WLAS/WAB Table E-8, Test Case 43
65	The device under test shall notify the user upon password expiration, but allow a specified additional number of subsequent logins within a specified time period before requiring a new password. The default for the number of subsequent logins shall not be greater than three. The default for the specified time period shall not be greater than 30 days.	UCR 2008: 5.4.6.2.1.2 (1.b.6.e, 1.b.6.e.1, and 1.b.6.e.2)		X	WLAS/WAB Table E-8, Test Cases 44-46
66	The device under test shall not hard code the notification mechanism for password expiration to allow for variation in variables such as "early warning period," "grace period," and subsequent login after password expiration.	UCR 2008: 5.4.6.2.1.2 (1.b.6.f)		X	WLAS/WAB Table E-8, Test Case 47
67	The device under test shall be capable of enforcing a configurable minimum period of waiting before an existing password can be updated (except for the first time update, which is required to be performed when the user logs in for the first time after being assigned a password). The default for the minimum waiting period shall be 24 hours without administrator intervention.	UCR 2008: 5.4.6.2.1.2 (1.b.7 and 1.b.7.a)		X	All Table E-8, Test Cases 48-49
68	The device under test shall be capable of ensuring that all user-entered passwords meet the following complexity requirements (so it cannot be "easily guessable"):	UCR 2008: 5.4.6.2.1.2 (1.b.8)		X	All Table E-8, Test Case 50
69	The device under test shall be capable of ensuring that all passwords including device under test security administrators, system administrators, and application administrator passwords consist of a mix of a minimum of 15 characters using at least two characters from each of the four character sets (i.e., upper-case letters, lower-case letters, numbers, and special characters).	UCR 2008: 5.4.6.2.1.2 (1.b.8.a and 1.b.8.b) & JTF-GNO Communications Tasking Order (CTO) 07-015		X	WLAS/WAB Table E-8, Test Cases 51-52

**Table 3-1. Wireless Products Capability/Functional Requirements Table
(continued)**

ID	Requirement	Reference	IO	IA	Remarks
IA Requirements Applicable to Wireless Components **("Test case" refers to the RTS IATP test case.)**				
70	The device under test shall be capable of ensuring that the password does not contain, repeat, or reverse the associated user-ID.	UCR 2008: 5.4.6.2.1.2 (1.b.8.c)		X	All Table E-8, Test Case 53
71	The device under test shall be capable of ensuring that the password does not contain three of the same characters used consecutively.	UCR 2008: 5.4.6.2.1.2 (1.b.8.d)		X	All Table E-8, Test Case 54
72	The device under test shall be capable of ensuring that a "null" password is not possible.	UCR 2008: 5.4.6.2.1.2 (1.b.8.e)		X	All Table E-8, Test Case 55
73	The device under test-supplied passwords shall be "reasonably" resistant to brute-force password guessing attacks. The total number of device under test-generated passwords shall be on the same order of magnitude as what a user could generate using the rules specified for user-entered passwords.	UCR 2008: 5.4.6.2.1.2 (1.b.9, 1.b.9.a, 1.b.9.b, 1.b.9.c) (Conditional)		X	All Table E-8, Test Cases 56-59
74	The device under test shall ensure that it does not prevent a user from choosing (e.g. unknowingly) a password that is already associated with another user-ID (Otherwise, an existing password may be divulged).	UCR 2008: 5.4.6.2.1.2 (1.b.10)		X	All Table E-8, Test Case 60
75	The device under test shall not permit passwords to be embedded in device under test defined access scripts or function keys.	UCR 2008: 5.4.6.2.1.2 (1.b.11)		X	All Table E-8, Test Case 61
76	The device under test shall have the capability to disable and enable the display of the "username of the last successful logon" feature.	UCR 2008: 5.4.6.2.1.2 (1.b.12)		X	All Table E-8, Test Case 62
77	If PINs are used for passwords, the device under test shall have a configurable parameter for the PIN length and the range shall be between four (4) and twenty (20) characters with a default of four (4).	UCR 2008: 5.4.6.2.1.2 (1.b.14) (Conditional)		X	All Table E-8, Test Case 64
78	If PINs are used for passwords, the device under test shall ensure that only numbers are allowed (i.e., no "#" or "*").	UCR 2008: 5.4.6.2.1.2 (1.b.14.a) (Conditional)		X	All Table E-8, Test Case 65
79	If PINs (User-ID) are used for user identification (versus password), the device under test shall be capable of ensuring that only one individual is permitted to use an assigned PIN.	UCR 2008: 5.4.6.2.1.2 (1.c) (Conditional)		X	All Table E-8, Test Case 66
80	If PINs (User-ID) are used for user identification, the device under test shall have a configurable length between six (6) and twenty (20) characters and the default shall be 6.	UCR 2008: 5.4.6.2.1.2 (1.c 1) (Conditional)		X	All Table E-8, Test Case 67
81	If PINs (User-ID) are used for user identification, the device under test shall only use numbers (i.e., no "#" or "*") when assigning the PIN (User-ID).	UCR 2008: 5.4.6.2.1.2 (1.c.2) (Conditional)		X	All Table E-8, Test Case 68

ID	Requirement	Reference	IO	IA	Remarks
IA Requirements Applicable to Wireless Components **("Test case" refers to the RTS IATP test case.)**				
82	The device under test shall be capable of supporting the unambiguity of a user-ID. This implies that the device under test shall prevent an appropriate administrator from creating (e.g., by mistake) a user-ID that already exists.	UCR 2008: 5.4.6.2.1.2 (1.d and 1.d.1)		X	All Table E-8, Test Cases 69-70
83	The device under test shall be capable of internally maintaining the identity of all user-IDs logged on at that time.	UCR 2008: 5.4.6.2.1.2 (1.e)		X	WLAS/WAB Table E-8, Test Case 71
84	The device under test shall be capable of associating a process that is invoked by a user or customer with the user-ID of that user.	UCR 2008: 5.4.6.2.1.2 (1.e.1)		X	WLAS/WAB Table E-8, Test Case 72
85	The device under test shall be capable of associating a process that is invoked by another process, with the ID of the invoking process.	UCR 2008: 5.4.6.2.1.2 (1.e.2)		X	WLAS/WAB Table E-8, Test Case 73
86	The device under test shall be capable of associating an autonomous processes (i.e., processes running without user or customer invocation) with an identification code (e.g., "system ownership").	UCR 2008: 5.4.6.2.1.2 (1.e.3)		X	WLAS/WAB Table E-8, Test Case 74
87	A device under test shall have the capability to disable (as distinct from deleting) a user-ID after a configurable specified time interval, if that user-ID has never been used during that time interval. This capability shall be either an autonomous disabling of the user-ID by the device under test, or an alarm/alert generated by the device under test for an appropriate administrator who then, depending on the policy, may disable the user-ID by using appropriate commands	UCR 2008: 5.4.6.2.1.2 (1.f and 1.f.1)		X	WLAS/WAB Table E-8, Test Cases 75-76
88	Disabled login ID shall not be re-enabled by the user or another application user.	UCR 2008: 5.4.6.2.1.2 (1.f.2)		X	WLAS/WAB Table E-8, Test Case 77
89	The device under test shall have the capability to configure the default time interval for disabling a user-ID that has not been used during that time interval. The default time interval shall be 90 days. In addition to disabling the user, the device under test is capable of sending an alert to the device under test's security administrator.	UCR 2008: 5.4.6.2.1.2 (1.g)		X	WLAS/WAB Table E-8, Test Case 78
90	The device under test shall be capable of verifying that a specified user (e.g., administrator) is only connected to the device under test a configurable number of times.	UCR 2008: 5.4.6.2.1.2 (1.h)		X	WLAS/WAB Table E-8, Test Case 79
91	Logon to the network a configurable number of times shall cause an alarm to be sent to the NMS unless an exception is granted per site policy.	UCR-2008: 5.4.6.2.1.2 (1.h.1)		X	WLAS/WAB Table E-8, Test Case 80

ID	Requirement	Reference	IO	IA	Remarks
IA Requirements Applicable to Wireless Components **("Test case" refers to the RTS IATP test case.)**
92	The device under test shall be capable of allowing the system security administrator to configure the number of consecutive failed logins for a user before the login procedure shall exit and end the attempted session. The number of times shall be between two and five and the default shall be three.	UCR 2008: 5.4.6.2.1.2 (1.i)		X	All Table E-8, Test Case 81
93	The device under test shall be capable of immediately notifying the user of a failed login (i.e., "Login Failed").	UCR 2008: 5.4.6.2.1.2 (1.i.1)		X	All Table E-8, Test Case 82
94	The device under test shall be capable of allowing a locked out user to be re-enabled by a configurable timer or manually by an application security administrator, a system administrator, or a system security administrator. Default for the lockout duration shall be configurable and the default shall be 60 seconds when the threshold for incorrect user-entered information has been exceeded.	UCR 2008: 5.4.6.2.1.2 (1.i.2. and 1.i.2.a)		X	All Table E-8, Test Cases 83-84
95	The device under test shall be capable of providing a mechanism to immediately notify (in real time) an appropriate administrator when the threshold for incorrect user-entered information is exceeded.	UCR 2008: 5.4.6.2.1.2 (1.i.3)		X	All Table E-8, Test Case 85
96	When the threshold for incorrect user-entered information has been exceeded, the device under test shall not, as a default arrangement, suspend the associated user-ID.	UCR 2008: 5.4.6.2.1.2 (1.i.4)		X	All Table E-8, Test Case 86
97	The device under test shall be capable of having different types of user roles. Note: Section 5.4.5.2.1, User Roles, defines the different types of user roles.	UCR 2008: 5.4.6.2.1.3 (1)		X	All Table E-8, Test Case 87
98	The device under test shall be capable of having at least three types of user roles: A system security administrator, a system administrator, and an application administrator.	UCR 2008: 5.4.6.2.1.3 (1.b)		X	WLAS/WAB Table E-8, Test Case 89
99	The device under test shall be capable of having at least three types of user roles: A system security administrator, a system administrator, and an application administrator.	UCR 2008: 5.4.6.2.1.3 (1.c)		X	WEI Table E-8, Test Case 90
100	The device under test shall be capable of setting the default user precedence VVoIP session origination capability as ROUTINE.	UCR 2008: 5.4.6.2.1.3 (1.d)		X	WEI Table E-8, Test Case 91
101	The device under test default user role shall be an application user.	UCR 2008: 5.4.6.2.1.3 (1.e)		X	WEI Table E-8, Test Case 92
102	The device under test default user role shall be a limited system administrator.	UCR 2008: 5.4.6.2.1.3 (1.f)		X	WLAS/WAB Table E-8, Test Case 93

Table 3-1. Wireless Products Capability/Functional Requirements Table (continued)

ID	Requirement	Reference	IO	IA	Remarks
IA Requirements Applicable to Wireless Components (**"Test case" refers to the RTS IATP test case.**)				
103	The device under test shall be capable of working properly without Super User access privileges for any user application roles (system security administrator, a system administrator, an application administrator, and application user).	UCR 2008:5.4.6.2.1.3 (1.g)		X	All Table E-8, Test Case 94
104	The device under test shall support appropriate system administrator functions as "separate" from other user functions.	UCR 2008: 5.4.6.2.1.3 (1.h)		X	All Table E-8, Test Case 95
105	The security functions performed by an appropriate administrator shall be identified and documented.	UCR 2008: 5.4.6.2.1.3 (1.h.1)		X	All Table E-8, Test Case 96
106	If the ability to enable or disable the administrator's account is an option of a device under test, the device under test shall not require that the account be enabled or activated during normal operation.	UCR 2008: 5.4.6.2.1.3 (1.h.2)		X	All Table E-8, Test Case 97
107	The Administrator shall have the capability to display all users currently logged onto the device under test.	UCR 2008: 5.4.6.2.1.3 (1.h.3); UCR 2008: 5.4.6.2.1.3 (1.h.3.a)		X	WLAS/WAB Table E-8, Test Cases 98-99
108	The Administrator shall have the capability to independently and selectively monitor (in real time) the actions of any one or more users, based on individual user identity.	UCR 2008: 5.4.6.2.1.3 (1.h.3.b)		X	WLAS/WAB Table E-8, Test Case 100
109	The Administrator shall have the capability to monitor the activities of a specific terminal, port, or network address in real time.	UCR 2008: 5.4.6.2.1.3 (1.h.3.c)		X	WLAS/WAB Table E-8, Test Case 101
110	The Administrator shall have the capability to authorize users.	UCR 2008: 5.4.6.2.1.3 (1.h.3.d)		X	WLAS/WAB Table E-8, Test Case 102
111	The Administrator shall have the capability to revoke users.	UCR 2008: 5.4.6.2.1.3 (1.h.3.e)		X	WLAS/WAB Table E-8, Test Case 103
112	The Administrator shall have the capability to lock out and restore a specific port or interface.	UCR 2008: 5.4.6.2.1.3 (1.h.3.f)		X	WLAS/WAB Table E-8, Test Case 104
113	The Administrator shall have the capability to identify all resources accessible to any specific user along with the associated privileges required to access them.	UCR 2008: 5.4.6.2.1.3 (1.h.3.g)		X	WLAS/WAB Table E-8, Test Case 105
114	The Administrator shall have the capability to deny the creation of a user-ID that is already in use.	UCR 2008: 5.4.6.2.1.3 (1.h.3.h)		X	WLAS/WAB Table E-8, Test Case 106
115	The Administrator shall have the capability to disable a user-ID after a specific period of time during which the user-ID has not been used.	UCR 2008: 5.4.6.2.1.3 (1.h.3.i)		X	WLAS/WAB Table E-8, Test Case 107
116	The Administrator shall have the capability to reinstate a disabled user-ID.	UCR 2008: 5.4.6.2.1.3 (1.h.3.j)		X	WLAS/WAB Table E-8, Test Case 108
117	The Administrator shall have the capability to delete a disabled user-ID.	UCR 2008: 5.4.6.2.1.3 (1.h.3.k)		X	WLAS/WAB Table E-8, Test Case 109
118	The Administrator shall have the capability to create or modify a password associated with a user-ID.	UCR 2008: 5.4.6.2.1.3 (1.h.3.l)		X	WLAS/WAB Table E-8, Test Case 110

Table 3-1. Wireless Products Capability/Functional Requirements Table (continued)

ID	Requirement	Reference	IO	IA	Remarks
IA Requirements Applicable to Wireless Components (**"Test case" refers to the RTS IATP test case.**)				
119	The Administrator shall have the capability to delete a user-ID along with its password.	UCR 2008: 5.4.6.2.1.3 (1.h.3.m)		X	WLAS/WAB Table E-8, Test Case 111
120	The Administrator shall have the capability to define a password-aging interval.	UCR 2008: 5.4.6.2.1.3 (1.h.3.n)		X	WLAS/WAB Table E-8, Test Case 112
121	The Administrator shall have the capability to define the interval during which an expired password of a user shall be denied reusing a password.	UCR 2008: 5.4.6.2.1.3 (1.h.3.o)		X	WLAS/WAB Table E-8, Test Case 113
122	The Administrator shall have the capability to define the events that may trigger an alarm, the levels of alarms, the type of notification, and the routing of the alarm.	UCR 2008: 5.4.6.2.1.3 (1.h.3.p)		X	WLAS/WAB Table E-8, Test Case 114
123	Define the events that may trigger an alarm, the levels of alarms, the type of notification, and the routing of the alarm.	UCR 2008: 5.4.6.2.1.3 (1.h.3.q)		X	WLAS/WAB Table E-8, Test Case 115
124	The Administrator shall have the capability to define the duration of session lock-out, which occurs when the threshold on the number of incorrect logins is exceeded.	UCR 2008: 5.4.6.2.1.3 (1.h.3.r)		X	WLAS/WAB Table E-8, Test Case 116
125	The Administrator shall have the capability to specify a customized advisory warning banner that is displayed upon valid test entry.	UCR 2008: 5.4.6.2.1.3 (1.h.3.s)		X	WLAS/WAB Table E-8, Test Case 117
126	The Administrator shall have the capability to define the duration of the time-out interval.	UCR 2008: 5.4.6.2.1.3 (1.h.3.t)		X	WLAS/WAB Table E-8, Test Case 118
127	The Administrator shall have the capability to define the privilege of a user to access a resource.	UCR 2008: 5.4.6.2.1.3 (1.h.3.u)		X	WLAS/WAB Table E-8, Test Case 119
128	The Administrator shall have the capability to define the privilege of an interface/port to be used to access a resource.	UCR 2008: 5.4.6.2.1.3 (1.h.3.v)		X	WLAS/WAB Table E-8, Test Case 120
129	The Administrator shall have the capability to permit post-collection audit analysis tools for report generation.	UCR 2008: 5.4.6.2.1.3 (1.h.3.w)		X	WLAS/WAB Table E-8, Test Case 121
130	The Administrator shall have the capability to permit the retrieval, copying, printing, or uploading of the security log.	UCR 2008: 5.4.6.2.1.3 (1.h.3.x)		X	WLAS/WAB Table E-8, Test Case 122
131	The Administrator shall have the capability to deny the ability to modify or delete the security log.	UCR 2008: 5.4.6.2.1.3 (1.h.3.y)		X	WLAS/WAB Table E-8, Test Case 123
132	The Administrator shall have the capability to provide a mechanism to specify the condition that would necessitate uploading the security log to avoid an overwrite in the buffer.	UCR 2008: 5.4.6.2.1.3 (1.h.3.z)		X	WLAS/WAB Table E-8, Test Case 124
133	The Administrator shall have the capability to provide a capability to validate the correct operation of the device under test.	UCR 2008: 5.4.6.2.1.3 (1.h.3.aa)		X	WLAS/WAB Table E-8, Test Case 125

ID	Requirement	Reference	IO	IA	Remarks
header: IA Requirements Applicable to Wireless Components ("Test case" refers to the RTS IATP test case.)					
134	The Administrator shall have the capability to provide a capability to monitor the device under test resources and their availabilities.	UCR 2008: 5.4.6.2.1.3 (1.h.3.bb)		X	WLAS/WAB Table E-8, Test Case 126
135	The Administrator shall have the capability to provide a capability to detect communication errors above an administrator- defined threshold.	UCR 2008: 5.4.6.2.1.3 (1.h.3.cc)		X	WLAS/WAB Table E-8, Test Case 127
136	The device under test shall only transmit passwords that are encrypted. Note: The Backbone Transport Services STIG requires that router administrative passwords are encrypted using MD5.	UCR 2008: 5.4.6.2.1.3 (1.j)		X	WLAS/WAB Table E-8, Test Case 129
137	The device under test shall be capable of limiting user access based on a time of day interval (i.e., duty hours).	UCR 2008: 5.4.6.2.1.3 (1.k)		X	WLAS/WAB Table E-8, Test Case 130
138	A device under test that uses ancillary AAA and syslog services shall do so in a secure manner.	UCR 2008: 5.4.6.2.1.4 (1) (Conditional)		X	All Table E-8, Test Case 131
139	A device under test that uses external Authentication, Authorization, and Accounting (AAA) services provided by the Diameter Base Protocol shall do so in accordance with RFC 3588.	UCR 2008:5.4.6.2.1.4 (1.a) (Conditional)		X	All Table E-8, Test Case 132
140	A device under test that acts as Diameter Agents shall be capable of being configured as Proxy Agents.	UCR 2008:5.4.6.2.1.4 (1.a.1) (Conditional)		X	All Table E-8, Test Case 133
141	A device under test that acts as Proxy Agents shall maintain session state.	UCR 2008: 5.4.6.2.1.4 (1.a.1.a) (Conditional)		X	All Table E-8, Test Case 134
142	All Diameter implementations shall ignore answers received that do not match a known Hop-by-Hop Identifier field.	UCR 2008: 5.4.6.2.1.4 (1.a.2) (Conditional)		X	All Table E-8, Test Case 135
143	All Diameter implementations shall provide transport of its messages in accordance with the transport profile described in RFC 3539.	UCR 2008: 5.4.6.2.1.4 (1.a.3) (Conditional)		X	All Table E-8, Test Case 136
144	A device under test that uses the Extensible Authentication Protocol (EAP) within Diameter shall do so in accordance with RFC 4072.	UCR 2008: 5.4.6.2.1.4 (1.a.4) (Conditional)		X	All Table E-8, Test Case 137
145	A device under test that uses external AAA services provided by the Remote Authentication Dial In User Service (RADIUS) shall do so in accordance with RFC 2865.	UCR 2008: 5.4.6.2.1.4 (1.b) (Conditional)		X	All Table E-8, Test Case 138
146	A device under test that uses the Extensible Authentication Protocol (EAP) within RADIUS shall do so in accordance with RFC 3579.	UCR 2008: 5.4.6.2.1.4 (1.b.1) (Conditional)		X	All Table E-8, Test Case 139
147	If the device under test supports RADIUS based accounting, it shall do so in accordance with RFC 2866.	UCR 2008: 5.4.6.2.1.4 (1.b.2) (Conditional)		X	All Table E-8, Test Case 140

ID	Requirement	Reference	IO	IA	Remarks
IA Requirements Applicable to Wireless Components ("Test case" refers to the RTS IATP test case.)				
148	If the device under test supports RADIUS, it shall support the use of IPSec and/or TLS using non-null transforms as defined in the confidentiality section of this UCR 2008 (Section 5.4.6, Requirements).	UCR 2008: 5.4.6.2.1.4 (1.b.3) (Conditional)		X	All Table E-8, Test Case 141
149	If the device under test supports RADIUS and IPSec, it shall support the use of IKE for key management as defined in the confidentiality section of this UCR 2008 (Section 5.4.6, Requirements).	UCR 2008: 5.4.6.2.1.4 (1.b.4) (Conditional)		X	All Table E-8, Test Case 142
150	A device under test that uses external AAA services provided by the Terminal Access Controller Access Control Device under test (TACACS+) shall do so in accordance with the TACACS+ Protocol Specification 1.78 (or later).	UCR 2008: 5.4.6.2.1.4 (1.c) Conditional)		X	All Table E-8, Test Case 143
151	If the device under test supports TACACS+, it shall support the use of IPSec and/or TLS using non-null transforms as defined in the confidentiality section (Section 5.4.6, Requirements).	UCR 2008: 5.4.6.2.1.4 (1.c.1) (Conditional)		X	All Table E-8, Test Case 144
152	If the device under test supports TACACS+ and IPSec, it shall support the use of IKE for key management as defined in the confidentiality section (Section 5.4.6, Requirements).	UCR 2008: 5.4.6.2.1.4 (1.c.2) (Conditional)		X	All Table E-8, Test Case 145
153	Devices under test that use external address assignment services provided by the DHCP shall do so in accordance with RFC 2131.	UCR 2008: 5.4.6.2.1.4 (1.d, 1.d.1, and 1.d.2) (Conditional)		X	WEI Table E-8, Test Cases146-148
154	A device under test that uses external AAA services provided by port based network access control mechanisms shall do so in accordance with IEEE 802.1X-2004 in combination with a secure Extensible Authentication Protocol (EAP) type (EAP-TLS, EAP-TTLS, or PEAP).	UCR 2008: 5.4.6.2.1.4 (1.e) (Conditional)		X	All Table E-8, Test Case 149
155	A device under test that uses external EAP services provided by EAP shall do so in accordance with RFC 3748 and its RFC extensions.	UCR 2008: 5.4.6.2.1.4 (1.e.1) (Conditional)		X	All Table E-8, Test Case 150
156	A device under test that supports EAP as a minimum shall support authentication using shared secrets. Note: RFC 3748 requires that devices under test support Identity, Notification, NAK, and MD-5 Challenge Request/Response exchanges.	UCR 2008: 5.4.6.2.1.4 (1.e.1.a) (Conditional)		X	All Table E-8, Test Case 151
157	Devices under test that use external syslog services shall do so in accordance with RFC 3164. Devices under test that support syslog shall use UDP port 514 for the source port of the sender when using UDP for transport.	UCR 2008: 5.4.6.2.1.4 (1.f, 1.f.1-1.f.3) (Conditional)		X	WLAS/WAB Table E-8, Test Cases 152-155

ID	Requirement	Reference	IO	IA	Remarks
IA Requirements Applicable to Wireless Components ("Test case" refers to the RTS IATP test case.)				
158	If the originally formed message has a TIMESTAMP in the HEADER part, then it shall be the local time of the device within its time zone. If the originally formed message has a HOSTNAME field, then it shall contain the hostname, as it knows itself. If it does not have a hostname, then it shall contain its own IP address. If the originally formed message has a TAG value, then it shall be the name of the program or process that generated the message	UCR 2008: 5.4.6.2.1.4 (1.f.3.a-1.f.3.c) (Conditional)		X	WLAS/WAB Table E-8, Test Cases 156-158
159	If devices under test use TCP for the delivery of syslog events, then the device under test shall do so in accordance with the RAW profile defined in RFC 3195.	UCR 2008: 5.4.6.2.1.4 (1.f.4) (Conditional)		X	WLAS/WAB Table E-8, Test Case 159
160	The device under test shall be capable of authenticating users and appliances.	UCR 2008: 5.4.6.2.1.5 (1)		X	All Table E-8, Test Case 160
161	The device under test shall only allow authenticated users and appliances to access the device under test. The device under test shall ensure those authentication credentials are not transmitted in the "clear" (i.e., credentials are encrypted end-to-end).	UCR 2008: 5.4.6.2.1.5 (1.a and 1.a.1)		X	All Table E-8, Test Cases 161-162
162	The device under test shall be capable of ensuring that device under test access points that provide remote login facility also provide authentication services that are capable of utilizing authentication mechanisms that are stronger than usernames and passwords, i.e., using two factor authentication (strong authentication).	UCR 2008: 5.4.6.2.1.5 (1.a.2)		X	WLAS/WAB Table E-8, Test Case 163
163	The device under test shall be capable of authenticating the LSC using TLS (or its equivalent) (Threshold) with PKI certificates.	UCR 2008: 5.4.6.2.1.5 (1.a.4)		X	WEI Table E-8, Test Case 165
164	The device under test shall be capable of authenticating an appliance using the DOD Public Key Infrastructure.	UCR 2008: 5.4.6.2.1.5 (1.b)		X	WLAS/WAB Table E-8, Test Case 166
165	If the device under test is PKE, then the device under test shall use the DOD PKI certificates with the associated public key in the TLS certificate message for authenticating appliance when using AS-SIP.	UCR 2008: 5.4.6.2.1.5 (1.b.1) (Conditional)			WEI Table E-8, Test Case 167

ID	Requirement	Reference	IO	IA	Remarks
IA Requirements Applicable to Wireless Components **("Test case" refers to the RTS IATP test case.)**					
166	A device under test shall be capable of ensuring that user authentication for logging in, logging, and auditing of an appliance shall be at least as strong as a user-ID and the appropriate password/PIN (user-ID) entered over a previously established trusted path.	UCR 2008: 5.4.6.2.1.5 (1.c)		X	WLAS/WAB Table E-8, Test Case 169
167	The device under test shall not support ways to bypass the deployed authentication mechanism.	UCR 2008: 5.4.6.2.1.5 (1.d)		X	All Table E-8, Test Case 170
168	The device under test shall perform the entire user authentication procedure even if the user-ID entered is not valid.	UCR 2008: 5.4.6.2.1.5 (1.e)		X	All Table E-8, Test Case 171
169	The device under test shall protect (i.e., encrypt) all internal storage of authentication data to ensure confidentiality.	UCR 2008: 5.4.6.2.1.5 (1.f)		X	All Table E-8, Test Case 172
170	The device under test shall be capable of allowing users to place ROUTINE precedence and emergency call without authenticating.	UCR 2008: 5.4.6.2.1.5 (1.g)		X	WEI Table E-8, Test Case 173
171	The device under test shall only allow authenticated users to access the device under test for services above the ROUTINE precedence	UCR 2008: 5.4.6.2.1.5 (1.h)		X	WEI Table E-8, Test Case 174
172	The device under test uses SIP, the device under test shall use digest authentication as specified in RFC 3261 and/or with PKI certificates for authenticating user credentials to the LSC through the EI. The user authentication mechanism shall be software enabled or disabled.	UCR 2008: 5.4.6.2.1.5 (1.h.1 and 1.h.2)		X	WEI Table E-8, Test Cases 175-176
173	If the device under test is a Softphone, the device under test shall provide user authentication by presenting the CAC credentials of the user to the LSC. The device under test shall only allow an authenticated system administrator to perform configuration functions.	UCR 2008: 5.4.6.2.1.5 (1.h.2.a and .b)		X	WEI Table E-8, Test Cases 177-178
174	The device under test shall not display configuration information without proper authentication.	UCR 2008: 5.4.6.2.1.5 (1.i)		X	WEI Table E-8, Test Case 179
175	The device under test shall be capable of ensuring that all ports on a device under test that support operations related command inputs (e.g., SNMP SET commands) exercise strong authentication mechanisms for access control.	UCR 2008: 5.4.6.2.1.5 (1.j)		X	WLAS/WAB Table E-8, Test Case 180
176	The device under test shall be capable of ensuring that all appliances that support connection-oriented communications also support mutual authentication between the requestor and the provider.	UCR 2008: 5.4.6.2.1.5 (1.k)		X	WLAS/WAB Table E-8, Test Case 181

Table 3-1. Wireless Products Capability/Functional Requirements Table (continued)

ID	Requirement	Reference	IO	IA	Remarks
IA Requirements Applicable to Wireless Components ("Test case" refers to the RTS IATP test case.)
177	The device under test shall properly operate when auto-registration is disabled	UCR 2008: 5.4.6.2.1.5 (1.l)		X	WEI Table E-8, Test Case 182
178	Default authentication mechanism for SNMPv3 shall be HMAC-SHA-96.	UCR 2008: 5.4.6.2.1.5 (1.m)		X	WLAS/WAB Table E-8, Test Case 183
179	The device under test shall be capable of meeting the DOD Public Key Enabled (PKE) requirements for PKI based authentication.	UCR 2008: 5.4.6.2.1.6 (1) and sub-paras (Conditional)		X	WEI Table E-8, Test Cases 184-231
180	The device under test shall be capable of providing authorization for services accessed on the device under test.	UCR 2008: 5.4.6.2.1.7 (1)		X	All Table E-8, Test Case 232
181	The device under test shall be capable of denying device under test access to any user unless identified with a user-ID and authenticated. Only authorized users shall be allowed access.	UCR 2008: 5.4.6.2.1.7 (1.a)		X	WLAS/WAB Table E-8, Test Case 233
182	The device under test shall be configured to not allow a user to access a resource unless that user's user-ID has an appropriate privilege to access that resource.	UCR 2008: 5.4.6.2.1.7 (1.b)		X	All Table E-8, Test Case 234
183	The device under test shall be capable of regulating remote access by employing positive technical controls such as proxies and screened subnets.	UCR 2008: 5.4.6.2.1.7 (1.c)		X	WLAS/WAB Table E-8, Test Case 236
184	The device under test shall be capable of configuring proxies and screened subnets to limit access to only approved, network service classes and configured traffic levels for the authenticated users and end instruments.	UCR 2008: 5.4.6.2.1.7 (1.d)		X	WLAS/WAB Table E-8, Test Case 237
185	The device under test shall have the capability of controlling the flow of traffic across an interface to the network based on the source/destination IP address, source/destination port number, DSCP, and protocol identifier ("6 tuple").	UCR 2008: 5.4.6.2.1.7 (1.d.1)		X	WLAS/WAB Table E-8, Test Case 238
186	The device under test shall be capable of utilizing VLANs to segregate VVoIP and data traffic. Servers requiring access to multiple VLANs shall be kept in a DMZ connected to the firewall and separating the two VLANs.	UCR 2008: 5.4.6.2.1.7 (1.d.2)		X	WLAS/WAB Table E-8, Test Case 242
187	The device under test shall be capable of supporting a minimum of five (5) distinct VLANs for VVoIP.	UCR 2008: 5.4.6.2.1.7 (1.d.2.a)		X	WLAS/WAB Table E-8, Test Case 243
188	The device under test shall be capable of ensuring that EIs (that do not contain a multi-port switch) and VVoIP appliances are only connected to switch ports with access to the VVoIP VLAN(s).	UCR 2008: 5.4.6.2.1.7 (1.d.2.b)		X	WLAS/WAB Table E-8, Test Case 244

Table 3-1. Wireless Products Capability/Functional Requirements Table (continued)

ID	Requirement	Reference	IO	IA	Remarks
IA Requirements Applicable to Wireless Components ("Test case" refers to the RTS IATP test case.)				
189	If the device under test supports a data workstation, then the device under test shall be capable of supporting 802.1Q trunking to separate VVoIP and data traffic or shall have a separate NIC for the data and the VVoIP.	UCR 2008: 5.4.6.2.1.7 (1.d.2.c) (Conditional)		X	WEI Table E-8, Test Case 245
190	If the device under test supports a data workstation, then the device under test shall be capable of using separate 802.1Q VLAN tags for VVoIP and data or shall use separate NICs for the data and VVoIP interfaces.	UCR 2008: 5.4.6.2.1.7 (1.d.2.c.i) (Conditional)		X	WEI Table E-8, Test Case 245
191	If the device under test supports a data workstation, then the device under test shall be capable of routing the VVoIP and data traffic to the appropriate VLAN.	UCR 2008: 5.4.6.2.1.7 (1.d.2.c.ii) (Conditional)		X	WEI Table E-8, Test Case 245
192	The device under test shall be capable of configuring the maximum number of MAC addresses that can be dynamically configured on a given switch port (e.g., 1-3).	UCR 2008: 5.4.6.2.1.7 (1.d.2.d)		X	WLAS/WAB Table E-8, Test Case 246
193	The device under test shall be capable of notifying the NMS when the MAC address table's threshold is reached to avoid an overflow.	UCR 2008: 5.4.6.2.1.7 (1.d.2.d.i)		X	WLAS/WAB Table E-8, Test Case 246
194	The device under test shall be capable of segregating soft phones to a dedicated VLAN.	UCR 2008: 5.4.6.2.1.7 (1.d.2.e)		X	WLAS/WAB Table E-8, Test Case 247
195	The device under test shall be capable of segregating flows to a dedicated VLAN.	UCR 2008: 5.4.6.2.1.7 (1.d.2.f -1.d.2.k)		X	WLAS/WAB Table E-8, Test Cases 248-253
196	The device under test shall have the capability to deploy on a dedicated IP network(s) or subnetwork(s) that utilize separate address blocks from the normal data address blocks thus allowing traffic and access control via firewalls and router ACLs.	UCR 2008: 5.4.6.2.1.7 (1.d.3)		X	WLAS/WAB Table E-8, Test Case 254
197	The device under test shall have the capability to be configured to ensure that the data network perimeter (i.e., data edge router or data perimeter firewall) blocks all external traffic destined to or sourced from the VVoIP VLANs and/or IP address space.	UCR 2008: 5.4.6.2.1.7 (1.d.3.b)		X	WLAS/WAB Table E-8, Test Case 260
198	The device under test shall have the capability to limit management appliance access to the IP addresses of appropriate workstations.	UCR 2008: 5.4.6.2.1.7 (1.d.3.c)		X	WLAS/WAB Table E-8, Test Case 261
199	If DHCP is used, the device under test shall have the capability to deploy different DHCP servers for VVoIP and non-VVoIP components, and the DHCP servers shall be located on physically diverse platforms from the routers and LAN switches.	UCR 2008: 5.4.6.2.1.7 (1.d.4) (Conditional)		X	WLAS/WAB Table E-8, Test Case 262

ID	Requirement	Reference	IO	IA	Remarks
IA Requirements Applicable to Wireless Components **("Test case" refers to the RTS IATP test case.)**				
200	If DHCP is used, the device under test shall be capable of using 802.1X in combination with a secure EAP type (EAPTLS, EAP-TTLS, or PEAP) residing on the authentication server and within the operating device under test or application software of the EI in order to authenticate to the LAN.	UCR 2008: 5.4.6.2.1.7 (1.d.5.and .5a) (Conditional)		X	WLAS/WAB Table E-8, Test Cases 263-264
201	If 802.1X port authentication is used, the device under test shall ensure that all access ports start in unauthorized state. Note: The device under test should set AuthControlledPortControl equal to Auto mode for ports that will support VVoIP.	UCR 2008 5.4.6.2.1.7 (1.d.5.a.i) (Conditional)		X	WLAS/WAB Table E-8, Test Case 265
202	If 802.1X port authentication is used, the device under test shall ensure that reauthentication occurs every 60 minutes.	UCR 2008 5.4.6.2.1.7 (1.d.5.a.ii) (Conditional)		X	All Table E-8, Test Case 266
203	If 802.1X port authentication is used the device under test shall also use 802.1AE and 802.1af to ensure a continuation of the authenticated relationship continues after the 802.1X authentication event to prevent parallel attacks.	UCR 2008 5.4.6.2.1.7 (1.d.5.a.iii) (Conditional)		X	All Table E-8, Test Case 267
204	The device under test documentation shall list all of the IP ports and protocols required by the device under test and the boundaries they transit as defined in the PPS Assurance Category Assignments List and which is maintained by DISA and is described in DODI 8551.1.	UCR 2008: 5.4.6.2.1.7 (1.e)		X	All Table E-8, Test Case 273
205	The device under test's shall not use IP ports and protocols deemed "red" as defined by the PPS Assurance Category Assignments List, which is maintained by DISA and is described in DODI 8551.1.	UCR 2008: 5.4.6.2.1.7 (1.e.1)		X	All Table E-8, Test Case 274
206	The device under test supports critical commands, operational commands or critical objects shall be capable of establishing access privileges for these objects and commands. Critical objects include authentication data storage.	UCR 2008: 5.4.6.2.1.7 (1.f)		X	WLAS/WAB Table E-8, Test Case 275
207	The default policy on a device under test that supports operations-related or critical commands shall be capable of disallowing command issuance unless the issuer has been authenticated and authorized to use that command.	UCR 2008: 5.4.6.2.1.7 (1.f.1)		X	WLAS/WAB Table E-8, Test Case 276

ID	Requirement	Reference	IO	IA	Remarks
IA Requirements applicable to wireless components **(test cases refer to RTS IATP test case)**
208	Assigning passwords to specific actions shall not be used as a primary access method	UCR 2008: 5.4.6.2.1.7 (1.f.1.a)		X	WLAS/WAB Table E-8, Test Case 277
209	All ports of the device under test that accept operations-related or critical command inputs shall be capable of exercising device under test access control. This includes ports that provide direct access, dial-up access, access via a wireless interface, network access, and access via a Data Communications Channel (DCC).	UCR 2008: 5.4.6.2.1.7 (1.f.2)		X	WLAS/WAB Table E-8, Test Case 278
210	Depending on the application, if the system is to be accessed by administrative users who need to keep this access (including the fact that an access is being made) confidential from other administrative users, such as unauthorized B/P/C/S Director of Information Management (DOIM) employees (i.e., CALEA type requirements), the system shall be capable of providing a separate interface/port for such confidential access and shall be capable of ensuring that messages (including login requests) at this "special" interface/port are kept confidential from users logged on at other interfaces/ports.	UCR 2008: 5.4.6.2.1.7 (1.f.2.a)		X	WLAS/WAB Table E-8, Test Case 279
211	The device under test shall be capable of controlling access to resources over a given interface/port on the basis of privileges assigned to that interface/port.	UCR 2008: 5.4.6.2.1.7 (1.f.2.b)		X	WLAS/WAB Table E-8, Test Case 280
212	The device under test shall have the capability of monitoring the flow of traffic across an interface to the network.	UCR 2008: 5.4.6.2.1.7 (1.g)		X	WLAS/WAB Table E-8, Test Case 281
213	The NMS shall possess read-access and limited write/controlled access capabilities unless Service/agency operational command personnel are available to make changes 24X7 to all DOD IP VVoIP database tables (excluding tables associated with non-DISA controlled devices).	UCR 2008: 5.4.6.2.1.7 (1.i)		X	WLAS/WAB Table E-8, Test Case 286

ID	Requirement	Reference	IO	IA	Remarks
IA Requirements applicable to wireless components (test cases refer to RTS IATP test case)				
214	If the device under test provides an emergency entry port (Emergency Action Interface) with device under test access control, the device under test shall have the capability to meet the requirements of using strong authentication; logging all access attempts in an audit log; and ensuring at least one, and not more than two, device under test security administrator accounts cannot be locked out due to login failures.	UCR 2008: 5.4.6.2.1.7 (1.l) (Conditional)		X	WLAS/WAB Table E-8, Test Case 290
215	The device under test shall be capable of using strong authentication.	UCR 2008: 5.4.6.2.1.7 (1.l.1)		X	WLAS/WAB Table E-8, Test Case 291
216	The device under test shall log all access attempts in an audit log.	UCR 2008: 5.4.6.2.1.7 (1.l.2)		X	WLAS/WAB Table E-8, Test Case 292
217	If the device under test provides an emergency entry port without device under test access control, then the following requirements shall be met: The device under test emergency entry port shall recognize only those commands that perform device under test restoration (for example, from a disk) and no other operations commands. The device under test shall generate a real time alarm/alert when this port is used to gain access to the device under test and transmit that alarm to the appropriate NOC.	UCR 2008: 5.4.6.2.1.7 (1.m, 1.m.1, and 1.m.2) (Conditional)		X	WLAS/WAB Table E-8, Test Cases 294-296
218	The device under test shall have the capability to deny the establishment of any session via a port that is not designed to accept operations-related command inputs. For example, if the output port receives a login request, the device under test shall not respond.	UCR 2008: 5.4.6.2.1.7 (1.n)		X	WLAS/WAB Table E-8, Test Case 297
219	The device under test shall be capable of providing a time-out feature for users of the device under test.	UCR 2008: 5.4.6.2.1.7 (1.o, 1.o.1-1.o.3)		X	WLAS/WAB Table E-8, Test Cases 298-301
220	The device under test shall be capable of providing a mechanism to end a user session through a secure logoff procedure.	UCR 2008: 5.4.6.2.1.7 (1.p)		X	WLAS/WAB Table E-8, Test Case 302

ID	Requirement	Reference	IO	IA	Remarks
IA Requirements applicable to wireless components **(test cases refer to RTS IATP test case)**
221	The device under test shall be capable of dropping a port if a session is interrupted due to reasons such as time-out, power failure, link disconnection, etc., and the same login procedure as described above shall be required of a subsequent session request.	UCR 2008: 5.4.6.2.1.7 (1.q)		X	WLAS/WAB Table E-8, Test Case 303
222	If the device under test employs external modems to perform dial/dial-back: (1) The modem, after receiving a call from a session requester, shall disconnect the line before dialing the authorized number to reestablish the contact. (2) The dial-back shall be performed over a line different from the line over which the session request arrived at the modem. (3) A loss of power to the modem shall not cause the modem to fall back to a default password. (4) The password file in the modem shall not be readable by a user. (5) The modem shall prevent any modification of its stored configuration unless the user attempting this modification is properly authenticated and found to be authorized for this action.	UCR 2008: 5.4.6.2.1.7 (1.r, 1.r.1-1.r.5) (Conditional)		X	WLAS/WAB Table E-8, Test Cases 304-309
223	The device under test shall be capable of limiting the access to newly created resources in conformance with the privilege of the creator of the resource. This should be the default configuration.	UCR 2008: 5.4.6.2.1.7 (1.s)		X	WLAS/WAB Table E-8, Test Case 310
224	If the application requires the device under test to provide different interfaces/ports for different functions, access to device under test resources over a given interface/port shall be controlled on the basis of privileges assigned to that interface/port.	UCR 2008: 5.4.6.2.1.7 (1.t) (Conditional)		X	WLAS/WAB Table E-8, Test Case 311
225	The device under test shall be capable of providing a level of granularity for any specified resource controlled by the device under test (to include precedence calls).	UCR 2008: 5.4.6.2.1.7 (1.u.1-1.u.8)		X	WLAS/WAB Table E-8, Test Cases 312-320
226	The device under test shall be capable of providing data and device under test integrity.	UCR 2008: 5.4.6.2.2 (1)		X	All Table E-9, Test Case 321
227	The device under test shall be capable of ensuring the integrity of signaling messages.	UCR 2008: 5.4.6.2.2 (1.a)			WEI Table E-9, Test Case 322
228	The device under test shall be capable of using TLS for providing integrity of AS-SIP messages. Note: The condition for the EI is the support of AS-SIP.	UCR 2008: 5.4.6.2.2 (1.a.1) (Conditional)		X	WEI Table E-9, Test Case 323

Table 3-1. Wireless Products Capability/Functional Requirements Table (continued)

ID	Requirement	Reference	IO	IA	Remarks
IA Requirements applicable to wireless components (test cases refer to RTS IATP test case)				
229	The device under test shall be capable of using HMAC-SHA1-160 with 160-bit keys.	UCR 2008: 5.4.6.2.2 (1.a.1.a) (Conditional)		X	WEI Table E-9, Test Case 324
230	If the device under test uses H.323, the system shall be capable of using H.235.1 Baseline Security Profile guidance for mutually authenticated shared keys and HMACSHA1-96 with 160-bit keys.	UCR 2008: 5.4.6.2.2 (1.a.2) (Conditional)		X	WEI Table E-9, Test Case 325
231	The device under test shall be capable of providing mechanisms to monitor system resources and their availabilities (e.g., overflow indication, lost messages, and buffer queues).	UCR 2008: 5.4.6.2.2 (1.d)		X	WLAS/WAB Table E-9, Test Case 335
232	The device under test shall be capable of providing mechanisms to detect communication errors (relevant to the system) above a specifiable threshold.	UCR 2008: 5.4.6.2.2 (1.e)		X	WLAS/WAB Table E-9, Test Case 336
233	The device under test shall be capable of providing data integrity of the bearer (Transport) packets.	UCR 2008: 5.4.6.2.2 (1.h)		X	WEI Table E-9, Test Case 339
234	The device under test shall be capable of using HMAC-SHA1-32 for the authentication tag, with 60-bit key length, as the default integrity mechanism for SRTP packets.	UCR 2008: 5.4.6.2.2 (1.h.1)		X	WEI Table E-9, Test Case 340
235	The device under test shall be capable of using HMAC-SHA1-80 for the authentication tag with 160-bit key length as the default integrity mechanism for SRTCP.	UCR 2008: 5.4.6.2.2 (1.h.2)		X	WEI Table E-9, Test Case 341
236	Devices that support remote network management functions and/or critical network resources and services shall be capable of providing appropriate standard (FIPS 140-2) cryptography-based data integrity services to protect and detect against unauthorized modification of messages	UCR 2008: 5.4.6.2.2 (1.i)		X	WLAS/WAB Table E-9, Test Case 342
237	The device under test and its applications shall be capable of ensuring that it cannot be made to enter an insecure state because of the operation of non-privileged code.	UCR 2008: 5.4.6.2.2 (1.j)		X	All Table E-9, Test Case 343
238	The device under test shall be capable of ensuring that default user-IDs and passwords, previously modified by the administrator, do not revert to the vendor-delivered default user-IDs and passwords when the device under test is restarted unless configured to do so by an appropriate administrator.	UCR 2008:5.4.6.2.2 (1.k)		X	All Table E-9, Test Case 344

ID	Requirement	Reference	IO	IA	Remarks
**IA Requirements applicable to wireless components** **(test cases refer to RTS IATP test case)**
239	The device under test shall be capable of providing mechanisms to ensure the integrity of the data that is stored on the appliance and is used to support authentication processes. This includes protecting the information from malicious deletion, modification, or insertion. Note: Examples of the data stored would be private keys or certificates.	UCR 2008:5.4.6.2.2 (1.l)		X	All Table E-9, Test Case 345
240	The entire SNMPv3 message shall be checked for integrity and shall use HMAC-SHA1-96 with 160-bit key length.	UCR 2008:5.4.6.2.2 (1.n)		X	WLAS/WAB Table E-9, Test Case 347
241	If the device under test uses SSHv2, the system shall use HMAC-SHA1- 96 with 160-bit key length for data integrity.	UCR 2008:5.4.6.2.2 (1.o)		X	WLAS/WAB Table E-9, Test Case 348
242	If the device under test uses TLS, the system shall be capable of using TLS (SSLv3.1 or higher) in combination with HMAC-SHA1-160 with 160-bit keys to provide integrity for session packets.	UCR 2008:5.4.6.2.2 (1.p) (Conditional)		X	WEI Table E-9, Test Case 349
243	The device under test shall be capable of providing data and signaling confidentiality for all VVoIP traffic.	UCR 2008: 5.4.6.2.3 (1)		X	WLAS/WAB Table E-10, Test Case 350
244	The device under test shall implement FIPS 140-2 Level 1 validated cryptographic hardware modules or software toolkits operated in FIPS Mode for all encryption mechanisms?	UCR 2008: 5.4.6.2.3 (1.a)		X	WLAS/WAB Table E-10, Test Case 351
245	The device under test shall be capable of providing confidentiality for media streams using SRTP with AES_CM_128 encryption algorithm as the default or [Required FY12] AES 256-bit algorithm.	UCR 2008: 5.4.6.2.3 (1.b)		X	WEI Table E-10, Test Case 352
246	The device under test shall be capable of generating keys using a random source algorithm that meets the requirements of FIPS 186 to support SRTP.	UCR 2008: 5.4.6.2.3 (1.b.1)		X	WEI Table E-10, Test Case 353
247	The device under test shall be capable of distributing the Master Key and the Salt Key in the VVoIP signaling messages.	UCR 2008: 5.4.6.2.3 (1.b.2)		X	WEI Table E-10, Test Case 354
248	The device under test shall be capable of distributing the Master Key and the Salt Key in concatenated form.	UCR 2008: 5.4.6.2.3 (1.b.3)		X	WEI Table E-10, Test Case 355
249	The device under test shall use a Master Key of 128 bits in order to support 128-bit AES encryption. Note: This implies that the Master Salt Key may be null.	UCR 2008: 5.4.6.2.3 (1.b.4)		X	WEI Table E-10, Test Case 356
250	The Master Key and a random Master Salt Key shall be supported for SRTP sessions. Note: This is in addition to the 256-bit requirement.	UCR 2008: 5.4.6.2.3 (1.b.5)		X	WEI Table E-10, Test Case 357

ID	Requirement	Reference	IO	IA	Remarks
IA Requirements applicable to wireless components **(test cases refer to RTS IATP test case)**				
251	The device under test shall be capable of providing confidentiality for signaling messages using TLS or IPSec using the AES 128-bit algorithm or AES 256-bit algorithm.	UCR 2008: 5.4.6.2.3 (1.c)		X	WEI Table E-10, Test Case 358
252	If H.323, MGCP, or H.248 (MEGACO) is used, the device under test shall be capable of using IPSec to provide confidentiality.	UCR 2008: 5.4.6.2.3 (1.c.1) (Conditional)		X	WEI Table E-10, Test Case 359
253	If IPSec is used, the device under test shall be capable of using Internet Key Exchange (IKE) for IPSec key distribution. [Required FY 10] IKE version 2. Note: IKEv2 requirements are found in UCR 2008, Section 5.3.5, IPv6 Requirements.	UCR 2008: 5.4.6.2.3 (1.c.1.c) (Conditional)		X	WEI Table E-10, Test Case 362
254	IKE version 1.	UCR 2008: 5.4.6.2.3 (1.c.1.c.i) (Conditional)		X	WEI Table E-10, Test Case 363
255	IKE version 2. Note: IKEv2 requirements are found in UCR 2008, Section 5.3.5, IPv6 Requirements.	UCR 2008: 5.4.6.2.3 (1.c.1.c.ii) (Conditional)		X	WEI Table E-10, Test Case 364
256	If IPSec is used, the device under test shall be capable of using the Revised Mode of public key encryption during Phase I of the ISAKMP negotiation for authentication.	UCR 2008: 5.4.6.2.3 (1.c.1.c.iii) (Conditional)		X	WEI Table E-10, Test Case 365
257	If IPSec is used, the device under test shall be capable of using the Quick Mode as the default Phase II authentication mechanism.	UCR 2008: 5.4.6.2.3 (1.c.1.c.iv) (Conditional)		X	WEI Table E-10, Test Case 366
258	If IPSec is used, the device under test shall be capable of using interpreting certificate requests for PKCS#7 wrapped certificates as a request for the whole path of certificates.	UCR 2008: 5.4.6.2.3 (1.c.1.c.v) (Conditional)		X	WEI Table E-10, Test Case 367
259	If IPSec is used, the system shall be capable of using Main Mode associated with the Diffie-Hellman approach for key generation for the security association negotiation.	UCR 2008: 5.4.6.2.3 (1.c.1.c.vi) (Conditional)		X	WEI Table E-10, Test Case 368
260	If IPSec is used, the device under test shall only support the following erroneous messages associated with a certificate request: Invalid key, Invalid ID, Invalid certificate encoding, Invalid certificate, Certificate type unsupported, Invalid CA, Invalid hash, Authentication failed, Invalid signature, Certificate unavailable.	UCR 2008: 5.4.6.2.3 (1.c.1.c.vi.a) (Conditional)		X	WEI Table E-10, Test Case 369
261	If IPSec is used, the device under test shall be capable of using Oakley Groups 1 and 2 as a minimum.	UCR 2008: 5.4.6.2.3 (1.c.1.c.vii) (Conditional)		X	WEI Table E-10, Test Case 370
262	If IPSec is used, the device under test shall be capable of using AES_128_CBC as the default encryption algorithm.	UCR 2008: 5.4.6.2.3 (1.c.1.d) (Conditional)		X	WEI Table E-10, Test Case 371

ID	Requirement	Reference	IO	IA	Remarks
	IA Requirements applicable to wireless components **(test cases refer to RTS IATP test case)**				
263	The device under test shall be capable of using TLS to provide confidentiality for the Assured Service- Session Initiation Protocol (AS-SIP). Note: The condition for the EI is the support of AS-SIP.	UCR 2008: 5.4.6.2.3 (1.c.2) (Conditional)		X	WEI Table E-10, Test Case 372
264	The underlying protocol for AS-SIP shall be the Transmission Control Protocol (TCP).	UCR 2008: 5.4.6.2.3 (1.c.2.a) (Conditional)		X	WEI Table E-10, Test Case 373
265	The device under test shall be capable of using as its default cipher either: [Conditional]TLS_RSA_WITH_AES_128_CBC_SHA or [Conditional, Required FY12] TLS_RSA_WITH_AES_256_CBC_SHA_	UCR 2008: 5.4.6.2.3 (1.c.2.b) (Conditional)		X	WEI Table E-10, Test Case 374
266	The device under test shall be capable of using a default of no compression for AS-SIP messages.	UCR 2008: 5.4.6.2.3 (1.c.2.c) (Conditional)		X	WEI Table E-10, Test Case 375
267	The device under test shall be capable of exchanging AS-SIP TLS messages in a single exchange or multiple exchanges	UCR 2008: 5.4.6.2.3 (1.c.2.d) (Conditional)		X	WEI Table E-10, Test Case 376
268	The device under test shall be capable of distributing the SRTP Master Key and Salt Key in the AS-SIP message using the SDP cryptofield. Note: EI condition is whether it supports AS-SIP.	UCR 2008: 5.4.6.2.3 (1.c.2.e) (Conditional)		X	WEI Table E-10, Test Case 377
269	If TLS session resumption is used, a timer associated with TLS session resumption shall be configurable and the default shall be one (1) hour. Note: This requirement is not associated with Network Management-related sessions.	UCR 2008: 5.4.6.2.3 (1.c.2.f) (Conditional)		X	WEI Table E-10, Test Case 378
270	The maximum time allowed for a TLS session to resume (session resumption) without repeating the TLS authentication/ confidentiality/authorization process is one (1) hour.	UCR 2008: 5.4.6.2.3 (1.c.2.f.i) (Conditional)		X	WEI Table E-10, Test Case 379
271	If AS-SIP is used, the device under test shall only transmit packets that are secured with TLS and use port 5061. Note: The systems may use other signaling protocols for interfacing to MGs, EIs, etc.	UCR 2008: 5.4.6.2.3 (1.c.2.g) (Conditional)		X	WEI Table E-10, Test Case 380
272	The device under test shall reflect all received AS-SIP packets associated with port 5061 that are not secured with TLS. Note: This ensures that the system does not process UDP, SCTP, and TCP SIP packets that are not secured using a combination of TLS and TCP.	UCR 2008: 5.4.6.2.3 (1.c.2.h) (Conditional)		X	WEI Table E-10, Test Case 381

ID	Requirement	Reference	IO	IA	Remarks
IA Requirements applicable to wireless components (test cases refer to RTS IATP test case)
273	The device under test shall be capable of using SSHv2 or TLS (SSLv3.1) or higher for remote configuration of appliances. Note: EIs remote manual configurations shall not be enabled and all non-automatic processes shall be performed locally.	UCR 2008: 5.4.6.2.3 (1.e) (Conditional)		X	WLAS/WAB Table E-10, Test Case 384
274	If the device under test uses SSH, the system shall do so in a secure manner, as defined by the following subtended requirements. Note: EIs remote manual configurations shall not be enabled and all no automatic processes shall be performed locally.	UCR 2008: 5.4.6.2.3 (1.g) (Conditional)		X	WLAS/WAB Table E-10, Test Case 391
275	If the device under test uses SSH, the system shall be capable of supporting the RSA 2,048-bit key algorithm.	UCR 2008: 5.4.6.2.3 (1.g.1) (Conditional)		X	WLAS/WAB Table E-10, Test Case 392
276	If the device under test uses SSH, the system shall use SSH in a secure manner.	UCR 2008: 5.4.6.2.3 (1.g.2) (Conditional)		X	WLAS/WAB Table E-10, Test Case 393
277	If the device under test uses SSH, a client shall close the session if it receives a request to initiate an SSH session whose version is less than 2.0.	UCR 2008: 5.4.6.2.3 (1.g.2.a) (Conditional)		X	WLAS/WAB Table E-10, Test Case 394
278	If the device under test uses SSH, SSH sessions shall re-key at a minimum of every 2^{31} of transmitted data or every 60 minutes, whichever comes first.	UCR 2008: 5.4.6.2.3 (1.g.2.b) (Conditional)		X	WLAS/WAB Table E-10, Test Case 395
279	If the device under test uses SSH, SSH sessions shall transmit less than 2^{32} packets after a key exchange has occurred.	UCR 2008: 5.4.6.2.3 (1.g.2.c) (Conditional)		X	WLAS/WAB Table E-10, Test Case 396
280	If the device under test uses SSH, SSH sessions shall re-key at a minimum after receiving 2^{31} packets or every 60 minutes, whichever comes first.	UCR 2008: 5.4.6.2.3 (1.g.2.d) (Conditional)		X	WLAS/WAB Table E-10, Test Case 397
281	If the device under test uses SSH, SSH sessions shall accept less than 2^{32} packets after a key exchange has occurred. Note: These requirements are consistent with the SSHv2 recommendation formula for the number of packets to accept ($2^{L/4}$ where L is the key length – 128 bits).	UCR 2008: 5.4.6.2.3 (1.g.2.e) (Conditional)		X	WLAS/WAB Table E-10, Test Case 398
282	If the device under test uses SSH, SSH sessions shall use as the default encryption algorithm either: AES 128-CBC or [conditional FY12] AES256-CBC.	UCR 2008: 5.4.6.2.3 (1.g.2.f) (Conditional)		X	WLAS/WAB Table E-10, Test Case 399
283	If the device under test uses SSH, SSH sessions shall use TCP as the underlying protocol.	UCR 2008: 5.4.6.2.3 (1.g.2.g) (Conditional)		X	WLAS/WAB Table E-10, Test Case 400
284	If the device under test uses SSH, the SSH packets shall have a configurable maximum uncompressed payload and the default shall be of 32, 768 bytes. This does not preclude the system from automatically sizing the MTU if it is less than 32,768.	UCR 2008: 5.4.6.2.3 (1.g.2.h) (Conditional)		X	WLAS/WAB Table E-10, Test Case 401

ID	Requirement	Reference	IO	IA	Remarks
**IA Requirements applicable to wireless components (test cases refer to RTS IATP test case)**
285	If the device under test uses SSH, SSH packets shall have a maximum packet size of 35,000 bytes including the packet_length, padding_length, payload, random padding, and mac.	UCR 2008: 5.4.6.2.3 (1.g.2.h.i) (Conditional)		X	WLAS/WAB Table E-10, Test Case 402
286	If the device under test uses SSH, the appliance shall discard SSH packets that exceed the maximum packet size to avoid denial of service attacks or buffer overflow attacks.	UCR 2008: 5.4.6.2.3 (1.g.2.h.ii) (Conditional)		X	WLAS/WAB Table E-10, Test Case 403
287	If the device under test uses SSH, SSH packets shall use random bytes if packet padding is required.	UCR 2008: 5.4.6.2.3 (1.g.2.h.iii) (Conditional)		X	WLAS/WAB Table E-10, Test Case 404
288	If the device under test uses SSH, the system shall treat all SSH encrypted packets sent in one direction as a single data stream. For example, the initialization vectors shall be passed from the end of one packet to the beginning of the next packet.	UCR 2008: 5.4.6.2.3 (1.g.2.i) (Conditional)		X	WLAS/WAB Table E-10, Test Case 405
289	If the device under test uses SSH, the system shall use Diffie-Hellman-Group2-SHA1 as the default key exchange mechanism for SSH.	UCR 2008: 5.4.6.2.3 (1.g.2.j) (Conditional)		X	WLAS/WAB Table E-10, Test Case 406
290	If the device under test uses SSH, the device using SSH shall be PKE and shall use the PKI to authenticate.	UCR 2008: 5.4.6.2.3 (1.g.2.k) (Conditional – FY12)		X	WLAS/WAB Table E-10, Test Case 407
291	If the device under test uses SSH, the device server using SSH shall have a host key.	UCR 2008: 5.4.6.2.3 (1.g.2.k.i) (Conditional – FY12)		X	WLAS/WAB Table E-10, Test Case 408
292	If the device under test uses SSH, the device shall certify and validate a server's host key using the DOD PKI before connecting with an SSH session.	UCR 2008: 5.4.6.2.3 (1.g.2.k.ii) (Conditional – FY12)		X	WLAS/WAB Table E-10, Test Case 409
293	If the device under test uses SSH, the device shall certify and validate a server's host key prior to connecting with an SSH session.	UCR 2008: 5.4.6.2.3 (1.g.2.k.iii) (Conditional – FY12)		X	WLAS/WAB Table E-10, Test Case 410
294	If the device under test uses SSH, the device shall disconnect a session if the authentication has not been accepted within 10 minutes.	UCR 2008: 5.4.6.2.3 (1.g.2.l) (Conditional)		X	WLAS/WAB Table E-10, Test Case 411
295	If the device under test uses SSH, the device shall disconnect if the number of failed authentication attempts for a single session exceeds a configurable parameter and the default shall be three attempts.	UCR 2008: 5.4.6.2.3 (1.g.2.m) (Conditional)		X	WLAS/WAB Table E-10, Test Case 412

ID	Requirement	Reference	IO	IA	Remarks
IA Requirements applicable to wireless components   **(test cases refer to RTS IATP test case)**
296	The device under test shall be capable of using SNMPv3 for all SNMP sessions. Note: If the device is using Version 1 or Version 2 (instead of SNMPv3) with all of the appropriate patches to mitigate the known security vulnerabilities, any findings associated with this requirement may be downgraded. In addition, if the device has also developed a migration plan to implement Version 3, any findings associated with this requirement may be further downgraded.	UCR 2008: 5.4.6.2.3 (1.h)		X	WLAS/WAB Table E-10, Test Case 413
297	The security level for SNMPv3 in the DOD VVoIP environment shall be authentication with privacy – snmpSecurityLevel=authPriv.	UCR 2008: 5.4.6.2.3 (1.h.1)		X	WLAS/WAB Table E-10, Test Case 414
298	The SNMPv3 architecture shall be capable of allowing an appropriate administrator to manually configure the snmpEngineID from the operator console. A default unique snmpEngineID may be assigned to avoid unnecessary administrative overhead, but this must be changeable.	UCR 2008: 5.4.6.2.3 (1.h.2)		X	WLAS/WAB Table E-10, Test Case 415
299	The security model for SMMPV3 shall be User-Based Security Model – snmpSecurity Model =3.	UCR 2008: 5.4.6.2.3 (1.h.3)		X	WLAS/WAB Table E-10, Test Case 416
300	If the device under test receives SNMP responses, the device shall conduct a timeliness check on the SNMPv3 message.	UCR 2008: 5.4.6.2.3 (1.h.3.a) (Conditional)		X	WLAS/WAB Table E-10, Test Case 417
301	An SNMPv3 engine shall perform time synchronization using authenticated messages.	UCR 2008: 5.4.6.2.3 (1.h.3.b)		X	WLAS/WAB Table E-10, Test Case 418
302	The message processing model shall be SNMPv3 – snmpMessage ProcessingModel=3.	UCR 2008: 5.4.6.2.3 (1.h.4)		X	WLAS/WAB Table E-10, Test Case 419
303	The default encryption cipher for SNMPv3 shall be CBC-DES-128 – usmDESPrivProtocol – CBCDES_128.	UCR 2008: 5.4.6.2.3 (1.h.5)		X	WLAS/WAB Table E-10, Test Case 420
304	If the device under test receives SNMP response messages, the SNMPv3 engine shall discard SNMP response messages that do not correspond to any current outstanding Request messages.	UCR 2008: 5.4.6.2.3 (1.h.6) (Conditional)		X	WLAS/WAB Table E-10, Test Case 421
305	If the device under test receives SNMP responses, the SNMPv3 Command Generator Application shall discard any Response Class PDU for which there is no outstanding Confirmed Class PDU.	UCR 2008: 5.4.6.2.3 (1.h.7) (Conditional)		X	WLAS/WAB Table E-10, Test Case 422

Table 3-1. Wireless Products Capability/Functional Requirements Table (continued)

ID	Requirement	Reference	IO	IA	Remarks
IA Requirements applicable to wireless components **(test cases refer to RTS IATP test case)**				
306	When using msgID for correlating Response messages to outstanding Request messages, the SNMPv3 engine shall use different msgIDs in all such Request messages that it sends out during a 150-second Time Window.	UCR 2008: 5.4.6.2.3 (1.h.8)		X	WLAS/WAB Table E-10, Test Case 423
307	An SNMPv3 command Generator or Notification Originator Application shall use different request-IDs in all Request PDUs that it sends out during a Time Window.	UCR 2008: 5.4.6.2.3 (1.h.9)		X	WLAS/WAB Table E-10, Test Case 424
308	When sending state altering messages to a managed authoritative SNMPv3 engine, a Command Generator Application should delay sending successive messages to that managed SNMPv3 engine until a positive acknowledgement is received from the previous message or until the message expires.	UCR 2008: 5.4.6.2.3 (1.h.10)		X	WLAS/WAB Table E-10, Test Case 425
309	The device under test using SNMPv3 shall implement the key-localization mechanism.	UCR 2008: 5.4.6.2.3 (1.h.11)		X	WLAS/WAB Table E-10, Test Case 426
310	The device under test shall be capable of using a separate interface for management traffic. Note: The separate interface may be a logically or physically separate interface.	UCR 2008: 5.4.6.2.3 (1.j)		X	WLAS/WAB Table E-10, Test Case 428
311	The device under test shall be capable of protecting the management interface using filters. Note: Within a router, the filters may be achieved using ACLs. Within an appliance, the filters may include internal routing procedures to the different physical interfaces or VLAN tagging.	UCR 2008: 5.4.6.2.3 (1.j.1)		X	WLAS/WAB Table E-10, Test Case 429
312	The device under test shall be capable of using VLANs to segregate management traffic from other types of traffic, where feasible. Note: The LS will implement the VLAN, but the other appliances will have to tag the packets with the correct VLAN tag.	UCR 2008: 5.4.6.2.3 (1.j.2)		X	WLAS/WAB Table E-10, Test Case 430
313	The device under test shall re-key each encrypted session once the session has transmitted a maximum of $2^{L/4}$ blocks of data. "L" is the block length in bits (e.g., 128 for AES_128) and shall be configurable. Note: This is to prevent birthday property and other modes of attack.	UCR 2008: 5.4.6.2.3 (1.m)		X	WLAS/WAB Table E-10, Test Case 433

ID	Requirement	Reference	IO	IA	Remarks
IA Requirements applicable to wireless components **(test cases refer to RTS IATP test case)**				
314	If the device under test is the originating party and receives a 181 message indicating that the call is being forwarded, then upon completion of the session establishment between the originating party and the forwarded-to party, the originating party must initiate a re-keying. Note: The re-keying is designed to prevent the forwarding party from having the key to the bearer session associated with the originating party and the forwarded-to party. If the forwarding party had the key to the bearer session, the forwarding party would be able to eavesdrop on the forwarded session. LSCs, MFSSs, and SSs may act as a B2BUA for an EI and would therefore originate the AS-SIP session on behalf of the EI.	UCR 2008: 5.4.6.2.3 (1.n) (Conditional)		X	WEI Table E-10, Test Case 434
315	If the EI acts as a bridge or an MCU, it shall establish a unique key for each EI connection.	UCR 2008: 5.4.6.2.3 (1.o) (Conditional)		X	WEI Table E-10, Test Case 435
316	The device under test shall be capable of providing non-repudiation and accountability services. Note: This assumes that authentication has already occurred as required previously.	UCR 2008: 5.4.6.2.4 (1)		X	WLAS/WAB Table E-11, Test Case 436
317	For user-accessible resources in the system that are created or modified by a user-ID via standard operations and maintenance procedures, the system shall be capable of providing a mechanism to identify the said user-ID, date, and time associated with the said resource creation or modification.	UCR 2008: 5.4.6.2.4 (1.a)		X	WLAS/WAB Table E-11, Test Case 437
318	The device under test shall be capable of auditing at the operating system and Database Management System (DBMS) levels and shall have a security log that contains information to support after the fact investigation of loss or impropriety and appropriate management response.	UCR 2008: 5.4.6.2.4 (1.b)		X	WLAS/WAB Table E-11, Test Case 438
319	The security log entry of any request or activity that is invoked by a user-ID shall be capable of including that user-ID so it becomes possible to establish user accountability. Note: The term "user-ID" shall be interpreted for this requirement to include users as well as processes.	UCR 2008: 5.4.6.2.4 (1.b.1)		X	WLAS/WAB Table E-11, Test Case 439
320	The security log shall be capable of protecting itself from unauthorized access or destruction.	UCR 2008: 5.4.6.2.4 (1.b.2)		X	WLAS/WAB Table E-11, Test Case 440

ID	Requirement	Reference	IO	IA	Remarks
IA Requirements applicable to wireless components **(test cases refer to RTS IATP test case)**				
321	The security log protection, at a minimum, shall be capable of providing access control based on user privileges and interface (logical or physical) privileges.	UCR 2008: 5.4.6.2.4 (1.b.2.a)		X	WLAS/WAB Table E-11, Test Case 441
322	The device under test shall have no mechanism for any external user (human or machine), including the administrator, to modify or delete the security log.	UCR 2008: 5.4.6.2.4 (1.b.2.b)		X	WLAS/WAB Table E-11, Test Case 442
323	The security log shall be capable of using a circular (or equivalent) recording mechanism (i.e., oldest record overwritten by newest).	UCR 2008: 5.4.6.2.4 (1.b.3)		X	WLAS/WAB Table E-11, Test Case 443
324	The device under test shall be capable of generating a security log alarm base upon specific conditions (e.g., percentage full by new entries since last upload, time interval elapsed since the last upload, disk space used). The alarm may necessitate uploading the security log (typically to some remote facility or other facility for long-term storage) to avoid an overwrite in the buffer. This upload may be automatically performed by the system or by an appropriate administrator.	UCR 2008: 5.4.6.2.4 (1.b.3.a)		X	WLAS/WAB Table E-11, Test Case 444
325	Only the system security administrator role shall have the ability to retrieve, print, copy, and upload the security log(s).	UCR 2008: 5.4.6.2.4 (1.b.4)		X	WLAS/WAB Table E-11, Test Case 445
326	The device under test shall be capable of ensuring security log copies maintain time sequentially and include all records stored in the security log up to the initiation of the copy.	UCR 2008: 5.4.6.2.4 (1.b.4.a)		X	WLAS/WAB Table E-11, Test Case 446
327	The device under test security log shall survive system restart (e.g. via reloading).	UCR 2008: 5.4.6.2.4 (1.b.5)		X	WLAS/WAB Table E-11, Test Case 447
328	The security log shall be capable of recording any action that changes the security attributes and services, access controls, or other configuration parameters of devices; each login attempt and its result; and each logout or session termination (whether remote or console), to include the following events by default as a minimum:	UCR 2008: 5.4.6.2.4 (1.b.6)		X	WLAS/WAB Table E-11, Test Case 448
329	Invalid user authentication attempt.	UCR 2008: 5.4.6.2.4 (1.b.6.a)		X	WLAS/WAB Table E-11, Test Case 449
330	Unauthorized attempts to access system resources.	UCR 2008: 5.4.6.2.4 (1.b.6.b)		X	WLAS/WAB Table E-11, Test Case 450
331	Changes made in a user's security profile and attributes.	UCR 2008: 5.4.6.2.4 (1.b.6.c)		X	WLAS/WAB Table E-11, Test Case 451
332	Changes made in security profiles and attributes associated with an interface/port.	UCR 2008: 5.4.6.2.4 (1.b.6.d)		X	WLAS/WAB Table E-11, Test Case 452

Table 3-1. Wireless Products Capability/Functional Requirements Table (continued)

ID	Requirement	Reference	IO	IA	Remarks
IA Requirements applicable to wireless components (test cases refer to RTS IATP test case)
333	Changes made in access rights associated with resources (i.e., privileges required of a user and an interface/ports to access).	UCR 2008: 5.4.6.2.4 (1.b.6.e)		X	WLAS/WAB Table E-11, Test Case 453
334	Changes made in system security configuration.	UCR 2008: 5.4.6.2.4 (1.b.6.f)		X	WLAS/WAB Table E-11, Test Case 454
335	Creation and modification of the system resources performed via standard operations and maintenance procedures.	UCR 2008: 5.4.6.2.4 (1.b.6.g)		X	WLAS/WAB Table E-11, Test Case 455
336	Disabling a user profile.	UCR 2008: 5.4.6.2.4 (1.b.6.h)		X	WLAS/WAB Table E-11, Test Case 456
337	Events associated with privileged users.	UCR 2008: 5.4.6.2.4 (1.b.6.i)		X	WLAS/WAB Table E-11, Test Case 457
338	If the device under test contains resources that are deemed mission critical (for example, a risk analysis classifies it critical), then the device should log any events associated with access to those mission critical resources.	UCR 2008: 5.4.6.2.4 (1.b.6.j)		X	WLAS/WAB Table E-11, Test Case 458
339	Successful login attempts.	UCR 2008: 5.4.6.2.4 (1.b.6.k)		X	WLAS/WAB Table E-11, Test Case 459
340	Failed login attempts, to include the following:	UCR 2008: 5.4.6.2.4 (1.b.6.l)		X	WLAS/WAB Table E-11, Test Case 460
341	Failed login attempt due to an excessive number of logon attempts.	UCR 2008: 5.4.6.2.4 (1.b.6.l.i)		X	WLAS/WAB Table E-11, Test Case 461
342	Failed logon attempt due to blocking or blacklisting of a user-ID.	UCR 2008: 5.4.6.2.4 (1.b.6.l.ii)		X	WLAS/WAB Table E-11, Test Case 462
343	Failed logon attempt due to blocking or blacklisting of a terminal.	UCR 2008: 5.4.6.2.4 (1.b.6.l.iii)		X	WLAS/WAB Table E-11, Test Case 463
344	Failed logon attempt due to blocking or blacklisting an access port.	UCR 2008: 5.4.6.2.4 (1.b.6.l.iv)		X	WLAS/WAB Table E-11, Test Case 464
345	The security log event record shall be capable of including at least the following information:	UCR 2008: 5.4.6.2.4 (1.b.7)		X	WLAS/WAB Table E-11, Test Case 465
346	Date and time of the event (both start and stop).	UCR 2008: 5.4.6.2.4 (1.b.7.a)		X	WLAS/WAB Table E-11, Test Case 466
347	User-ID including associated terminal, port, network address, or communication device.	UCR 2008: 5.4.6.2.4 (1.b.7.b)		X	WLAS/WAB Table E-11, Test Case 467
348	Event type.	UCR 2008: 5.4.6.2.4 (1.b.7.c)		X	WLAS/WAB Table E-11, Test Case 468
349	Names of resources accessed.	UCR 2008: 5.4.6.2.4 (1.b.7.d)		X	WLAS/WAB Table E-11, Test Case 469
350	Success or failure of the event.	UCR 2008: 5.4.6.2.4 (1.b.7.e)		X	WLAS/WAB Table E-11, Test Case 470
351	The device under test shall have the capability to notify (e.g., via critical alarm, alert, or online report), within 30 seconds, an appropriate Networks Operations Center (NOC) if the security log fails to record the events that are required to be recorded.	UCR 2008: 5.4.6.2.4 (1.b.8)		X	WLAS/WAB Table E-11, Test Case 471
352	The device under test shall not record actual or attempted passwords in the security log.	UCR 2008: 5.4.6.2.4 (1.b.9)		X	WLAS/WAB Table E-11, Test Case 472

ID	Requirement	Reference	IO	IA	Remarks
IA Requirements applicable to wireless components (test cases refer to RTS IATP test case)				
353	The device under test shall ensure that security and audit logs are maintained separate from other audit logs (history or CDR audit logs).	UCR 2008: 5.4.6.2.4 (1.b.10)		X	WLAS/WAB Table E-11, Test Case 473
354	The device under test shall ensure that security and audit logs are maintained separate from other audit logs (history or CDR audit logs).	UCR 2008: 5.4.6.2.4 (1.b.11)		X	WLAS/WAB Table E-11, Test Case 474
355	If the device under test accesses other systems to pass on a request or activity that has a user-ID associated with it, the device shall have the capability to make that user-ID available to other systems. Thus, if the other systems have the capability to accept the user-ID information, the said user can be traceable for the lifetime of the request or activity.	UCR 2008: 5.4.6.2.4 (1.c)		X	WLAS/WAB Table E-11, Test Case 475
356	The device under test shall be capable of providing post-collection audit analysis tools that can produce typical reports (e.g., exception reports, summary reports, and detailed reports) on specific data items, users, or communication facilities.	UCR 2008: 5.4.6.2.4 (1.d)		X	WLAS/WAB Table E-11, Test Case 476
357	The VVoIP device under test shall meet the availability requirements as stated in the UCR 2008, Section 5.3.2.2.3.8, System Quality Factors. There is additional IA specific IA availability requirements specified below that are not covered in the System Quality Factors section of the UCR.	UCR 2008: 5.4.6.2.5 (1)		X	WLAS/WAB Table E-12, Test Case 477
358	The system shall have robustness through the maximum use of alternative routing, backup. Note: From a vendor's perspective, this requirement is associated with meeting the reliability numbers for the system.	UCR 2008: 5.4.6.2.5 (1.a)		X	WLAS/WAB Table E-12, Test Case 478
359	The device under test shall have mechanisms to allow "secure recovery" to reduce vulnerability due to failure or discontinuity making it vulnerable to security compromise. Note: This requirement will ensure that as a device is reestablished, it does not reboot in an unsecured mode such as with factory set configurations.	UCR 2008: 5.4.6.2.5 (1.b)		X	WLAS/WAB Table E-12, Test Case 479
360	The device under test shall have the capability to rebuild the device to a base version and subsequent vendor modification of that version, if that version and modification are currently in use.	UCR 2008: 5.4.6.2.5 (1.c)		X	WLAS/WAB Table E-12, Test Case 480

ID	Requirement	Reference	IO	IA	Remarks
IA Requirements applicable to wireless components **(test cases refer to RTS IATP test case)**				
361	The device under test shall have the capability to provide adequate checkpoints in a process flow of the software system so that, upon detection of service deterioration, a recovery to an acceptable level is facilitated.	UCR 2008: 5.4.6.2.5 (1.d)		X	WLAS/WAB Table E-12, Test Case 481
362	The device under test shall have a capability to define a threshold e.g., percentage full by new entries since last upload, time interval elapsed since last upload to initiate a warning before a security log buffer overflow.	UCR 2008: 5.4.6.2.5 (1.e)		X	WLAS/WAB Table E-12, Test Case 482
IPv6 Requirements Applicable to Wireless Components				
363	The device under test shall support dual IPv4 and IPv6 stacks as described in RFC 4213.	UCR 2008: 5.3.5.3 (1)	X	X	WLAS/WAB Conditional -WEI Table E-13, Test Case 1 TP IO-26
364	If the device under test supports routing functions, the device shall support the manual tunnel requirements as described in RFC 4213.	UCR 2008: 5.3.5.3 (1.1) (Conditional)		X	WLAS/WAB Table E-13, Test Case 2
365	The device under test shall support the IPv6 format as described in RFC 2460 and updated by RFC 5095.	UCR 2008: 5.3.5.3 (2)	X	X	All Table E-13, Test Case 3 TP IO-27
366	The device under test shall support the transmission of IPv6 packets over Ethernet networks using the frame format defined in RFC 2464.	UCR 2008: 5.3.5.3 (3)	X	X	All Table E-13, Test Case 4 TP IO-28
367	The device under test shall support Path Maximum Transmission Unit (MTU) Discovery (RFC 1981).	UCR 2008: 5.3.5.3.1 (4)		X	WLAS/WAB Conditional -WEI Table E-13, Test Case 5
368	The device under test shall support a minimum MTU of 1280 bytes (RFC 2460 and updated by RFC 5095).	UCR 2008: 5.3.5.3.1 (5)		X	All Table E-13, Test Case 6
369	If Path MTU Discovery is used and a "Packet Too Big" message is received requesting a next-hop MTU that is less than the IPv6 minimum link MTU, the device shall ignore the request for the smaller MTU and shall include a fragment header in the packet.	UCR 2008: 5.3.5.3.1 (6) (Conditional)		X	All Table E-13, Test Case 7
370	The device under test shall not use the Flow Label field as described in RFC 2460.	UCR 2008: 5.3.5.3.2 (7)		X	WEI Table E-13, Test Case 8
371	The device under test shall be capable of setting the Flow Label field to zero when originating a packet.	UCR 2008: 5.3.5.3.2 (7.1)		X	WEI Table E-13, Test Case 9
372	The device under test shall not modify the Flow Label field when forwarding packets.	UCR 2008: 5.3.5.3.2 (7.2)		X	WEI Table E-13, Test Case 10
373	The device under test shall be capable of ignoring the Flow Label field when receiving packets.	UCR 2008: 5.3.5.3.2 (7.3)		X	WEI Table E-13, Test Case 11
374	The device under test shall support the IPv6 Addressing Architecture as described in RFC 4291.	UCR 2008: 5.3.5.3.3 (8)	X	X	All Table E-13, Test Case 12 TP IO-29

ID	Requirement	Reference	IO	IA	Remarks
IPv6 Requirements Applicable to Wireless Components
375	The device under test shall support the IPv6 Scoped Address Architecture as described in RFC 4007.	UCR 2008: 5.3.5.3.3 (9)	X		All TP IO-30
376	If a scoped address (RFC 4007) is used, the device shall use a scope index value of zero (0) when the default zone is intended.	UCR 2008: 5.3.5.3.3 (9.1)	X		All TP IO-31
377	If a scoped address (RFC 4007) is used, the device shall use the syntax of <address>%<zone_id>/<prefix_length> when specifying an IPv6 non-global address. Note: "Address" is the IPv6 address and % and / are delimiters. If the zone id is zero (0) or default, the % and zone id may be omitted.	UCR 2008: 5.3.5.3.3 (9.2)	X		All TP IO-32
378	If Dynamic Host Configuration Protocol (DHCP) is supported within an IPv6 system, it shall be implemented in accordance with the DHCP for IPv6 (DHCPv6) as described in RFC 3315.	UCR 2008: 5.3.5.3.3 (10) (Conditional)		X	All Table E-13, Test Case 13
379	If the device under test is a DHCPv6 client, the device shall discard any messages that contain options that are not allowed, which are specified in Section 15 of RFC 3315.	UCR 2008: 5.3.5.3.3 (10.1) (Conditional)		X	WEI Table E-13, Test Case 14
380	The device under test shall support DHCPv6 as described in RFC 3315. Note: The following subtended requirements are predicated upon an implementation of DHCPv6 for the end instrument. It is not expected that other UC appliances will use DHCPv6.	UCR 2008: 5.3.5.3.3 (10.2)		X	WEI Table E-13, Test Case 15
381	If the device under test is a DHCPv6 client, and the first Retransmission Timeout has elapsed since the client sent the Solicit message and the client has received an Advertise message(s), but the Advertise message(s) does not have a preference value of 255, the client shall continue with a client-initiated message exchange by sending a Request message.	UCR 2008: 5.3.5.3.3 (10.2.1)		X	WEI Table E-13, Test Case 16
382	If the device under test is a DHCPv6 client and the DHCPv6 message exchange fails, it shall restart the reconfiguration process after receiving user input, system restart, attachment to a new link, a device configurable timer, or a user defined external event occurs. Note: The intent is to ensure that the DHCP client continues to restart the configuration process periodically until it succeeds.	UCR 2008: 5.3.5.3.3 (10.2.2)		X	WEI Table E-13, Test Case 17
383	If the device under test is a DHCPv6 client and it sends an Information-Request message, it shall include a Client Identifier option to allow it to be authenticated to the DHCPv6 server.	UCR 2008: 5.3.5.3.3 (10.2.3)		X	WEI Table E-13, Test Case 18

Table 3-1. Wireless Products Capability/Functional Requirements Table (continued)

ID	Requirement	Reference	IO	IA	Remarks
	IPv6 Requirements Applicable to Wireless Components				
384	If the device under test is a DHCPv6 client, it shall perform duplicate address detection upon receipt of an address from the DHCPv6 server prior to transmitting packets using that address for itself.	UCR 2008: 5.3.5.3.3 (10.2.4)		X	WEI Table E-13, Test Case 19
385	If the device under test is a DHCPv6 client, it shall log all reconfigure events.	UCR 2008: 5.3.5.3.3 (10.2.5)		X	WEI Table E-13, Test Case 20
386	If the device under test supports DHCPv6 and uses authentication, it shall discard unauthenticated DHCPv6 messages from UC systems and log the event. Note: This requirement assumes authentication is used as described in RFC 3118 (and extended in RFC 3315) but does not require authentication.	UCR 2008: 5.3.5.3.3 (10.3) (Conditional)		X	All Table E-13, Test Case 21
387	The device under test shall support Neighbor Discovery for IPv6 as described in RFC 2461 and RFC 4861 (FY10).	UCR 2008: 5.3.5.3.5 (11)	X	X	All Table E-13, Test Case 22 TP IO-33
388	The device under test shall not set the override flag bit in the neighbor advertisement message for solicited advertisements for anycast addresses or solicited proxy advertisements.	UCR 2008: 5.3.5.3.5 (11.1)		X	All Table E-13, Test Case 23
389	The device under test shall set the override flag bit in the neighbor advertisement message to "1" if the message is not an anycast address or a unicast address for which the device is providing proxy service.	UCR 2008: 5.3.5.3.5 (11.2)		X	All Table E-13, Test Case 24
390	If a valid neighbor advertisement is received by the device and the device neighbor cache does not contain the target's entry, the advertisement shall be silently discarded.	UCR 2008: 5.3.5.3.5 (11.3) (Conditional)		X	All Table E-13, Test Case 25
391	If a valid neighbor advertisement is received by the device under test and the device neighbor cache entry is in the INCOMPLETE state when the advertisement is received and the link layer has addresses and no target link-layer option is included, the device under test shall silently discard the received advertisement.	UCR 2008: 5.3.5.3.5 (11.4) (Conditional)		X	All Table E-13, Test Case 26
392	If address resolution fails on a neighboring address, the entry shall be deleted from the device under test's neighbor cache.	UCR 2008: 5.3.5.3.5 (11.5) (Conditional)		X	All Table E-13, Test Case 27
393	The device under test shall support the ability to configure the system to ignore redirect messages.	UCR 2008: 5.3.5.3.5 (11.6)		X	WEI Table E-13, Test Case 28
394	The device under test shall only accept redirect messages from the same router as is currently being used for that destination.	UCR 2008: 5.3.5.3.5.1 (11.7)		X	All Table E-13, Test Case 29

ID	Requirement	Reference	IO	IA	Remarks
IPv6 Requirements Applicable to Wireless Components				
395	If redirect messages are allowed, the device under test shall update its destination cache in accordance with the validated redirect message.	UCR 2008: 5.3.5.3.5.1 (11.7.1) (Conditional)		X	All Table E-13, Test Case 30
396	If the valid redirect message is allowed and no entry exists in the destination cache, the device under test shall create an entry.	UCR 2008: 5.3.5.3.5.1 (11.7.2) (Conditional)		X	All Table E-13, Test Case 31
397	If the device under test sends router advertisements, the device shall inspect valid router advertisements sent by other routers and verify that the routers are advertising consistent information on a link and shall log any inconsistent router advertisements.	UCR 2008: 5.3.5.3.5.2 (11.8) (Conditional)		X	WLAS/WAB Table E-13, Test Case 32
398	The device under test shall prefer routers that are reachable over routers whose reachability is suspect or unknown.	UCR 2008: 5.3.5.3.5.2 (11.8.1)		X	WEI Table E-13, Test Case 33
399	If the device under test sends router advertisements, the device shall include the MTU value in the router advertisement message for all links in accordance with RFC 2461 and RFC 4861 (FY2010).	UCR 2008: 5.3.5.3.5.2 (11.9) (Conditional)		X	WLAS/WAB Table E-13, Test Case 34
400	If the device under test supports stateless IP address autoconfiguration, the device shall support IPv6 Stateless Address Auto- Configuration (SLAAC) for interfaces supporting UC functions in accordance with RFC 2462 and RFC 4862 (FY2010).	UCR 2008: 5.3.5.3.6 (12)		X	All (Softphone only) Table E-13, Test Case 35
401	The device under test shall have a configurable parameter that allows the "managed address configuration" flag and the "other stateful configuration" flag to always be set and not perform stateless auto configuration.	UCR 2008: 5.3.5.3.6 (12.1)		X	All Table E-13, Test Case 36
402	The device under test shall support manual assignment of IPv6 addresses.	UCR 2008: 5.3.5.3.6 (12.2)		X	All Table E-13, Test Case 37
403	The device under test shall support stateful autoconfiguration (i.e., ManagedFlag=TRUE). Note: This requirement is associated with the earlier requirement for the EI to support DHCPv6.	UCR 2008: 5.3.5.3.6 (12.3)		X	WEI Table E-13, Test Case 38
404	If the device under test sends router advertisements, the device shall default to using the "managed address configuration" flag and the "other stateful flag" set to TRUE in their router advertisements when stateful autoconfiguration is implemented.	UCR 2008: 5.3.5.3.6 (12.3.1) (Conditional)		X	WLAS/WAB Table E-13, Test Case 39

ID	Requirement	Reference	IO	IA	Remarks
IPv6 Requirements Applicable to Wireless Components
405	If the device under test supports a subtended appliance behind it, the device shall ensure that the IP address assignment process of the subtended appliance is transparent to the UC components of the system and does not cause the device to attempt to change its IP address. Note: An example is a PC that is connected to the LAN through the hub or switch interface on a phone. The address assignment process of the PC should be transparent to the EI and should not cause the phone to attempt to change its IP address.	UCR 2008: 5.3.5.3.6 (12.4) (Conditional)		X	EI Table E-13, Test Case 40
406	If the device under test supports IPv6 SLAAC, the device shall have a configurable parameter that allows the function to be enabled and disabled.	UCR 2008: 5.3.5.3.6 (12.5) (Conditional)		X	EI Table E-13, Test Case 41
407	If the device under test supports SLAAC, and security constraints prohibit the use of hardware identifiers as part of interface addresses generated using SLAAC, IPSec-capable systems shall support privacy extensions for stateless address autoconfiguration as defined in RFC 4941 - Privacy Extensions for Stateless Address Autoconfiguration in IPv6.	UCR 2008: 5.3.5.3.6 (12.6) (Conditional -Softphones)		X	EI Table E-13, Test Case 42
408	If the device under test supports stateless IP address autoconfiguration, the device shall support a configurable parameter to enable or disable manual configuration of the site-local and Global addresses (i.e., disable the "Creation of Global and Site-Local Addresses" as described in Section 5.5 of RFC 2462).	UCR 2008: 5.3.5.3.6 (12.7)		X	All WEI-Softphone Table E-13, Test Case 43
409	IPv6 nodes shall support link-local address configuration, and the Duplicate Address Detection (DAD) shall not be disabled in accordance with RFC 2462 and RFC 4862 (FY2010).	UCR 2008: 5.3.5.3.6 (12.8)		X	All Table E-13, Test Case 44
410	The device under test shall support the Internet Control Message Protocol for IPv6 (ICMPv6) as described in RFC 4443.	UCR 2008: 5.3.5.3.7 (14)	X	X	All Table E-13, Test Case 45 TP IO-34
411	The device under test shall have a configurable rate limiting parameter for rate limiting the forwarding of ICMP messages.	UCR 2008: 5.3.5.3.7 (14.1)	X	X	All Table E-13, Test Case 46 TP IO-35
412	The device under test shall support the capability to enable or disable the ability of the device to generate a Destination Unreachable message in response to a packet that cannot be delivered to its destination for reasons other than congestion.	UCR 2008: 5.3.5.3.7 (14.2)	X	X	All Table E-13, Test Case 47 TP IO-36

ID	Requirement	Reference	IO	IA	Remarks
	IPv6 Requirements Applicable to Wireless Components				
413	The device under test shall support the enabling or disabling of the ability to send an Echo Reply message in response to an Echo Request message sent to an IPv6 multicast or anycast address.	UCR 2008: 5.3.5.3.7 (14.3)		X	All Table E-13, Test Case 48
414	The device under test shall validate ICMPv6 messages, using the information contained in the payload, prior to acting on them.	UCR 2008: 5.3.5.3.7 (14.4)		X	All Table E-13, Test Case 49
415	If the device under test supports routing functions, the device shall support the Open Shortest Path First (OSPF) for IPv6 as described in RFC 2740.	UCR 2008: 5.3.5.3.8 (15) (Conditional)	X	X	WLAS/WAB Table E-13, Test Case 50 TP IO-37
416	If the device under test supports routing functions, the device shall support securing OSPF with Internet Protocol Security (IPSec) as described for other IPSec instances in UCR 2008, Section 5.4, and Information Assurance.	UCR 2008: 5.3.5.3.8 (15.1) (Conditional)		X	WLAS/WAB Table E-13, Test Case 51
417	If the device under test supports routing functions, the device shall support router-to-router integrity using the IP Authentication Header with HMAC-SHA1-128 as described in RFC 4302.	UCR 2008: 5.3.5.3.8 (15.2) (Conditional)		X	WLAS/WAB Table E-13, Test Case 52
418	If the device under test supports routing functions, the system shall support the Multicast Listener Discovery (MLD) process as described in RFC 2710 and extended in RFC 3810. Note: The FY 2008 VVoIP design does not utilize multicast, but routers supporting VVoIP also support data applications that may utilize multicast. A Softphone will have non-routing functions that require MLDv2	UCR 2008: 5.3.5.3.8 (20)		X	EI-Softphone Conditional-WLAS/WAB Table E-13, Test Case 58
419	The device under test shall support MLD as described in RFC 2710. Note: This requirement was added in order to ensure that Neighbor Discovery multicast requirements are met. Routers are not included in this requirement since they have to meet RFC 2710 in the preceding requirement.	UCR 2008: 5.3.5.3.8 (21)		X	All Table E-13, Test Case 59
420	If the device under test uses IPSec, the device shall support the Security Architecture for the IP RFC 2401 and RFC 4301 (FY2010). In FY08, RFC 2401 (and its related RFCs) is the Threshold requirement as described in UCR 2008, Section 5.4, Information Assurance. In addition, the interfaces required to use IPSec are defined in UCR 2008, Section 5.4, Information Assurance.	UCR 2008: 5.3.5.3.8 (22)		X	EI-Softphone Conditional –WLAS/WAB Table E-13, Test Case 60

ID	Requirement	Reference	IO	IA	Remarks
IPv6 Requirements Applicable to Wireless Components
421	If RFC 4301 is supported, the device under test shall support binding of a security association (SA) with a particular context.	UCR 2008: 5.3.5.3.8 (22.1)		X	EI-Softphone Conditional –WLAS/WAB Table E-13, Test Case 61
422	If RFC 4301 is supported, the device under test shall be capable of disabling the BYPASS IPSec processing choice. Note: The intent of this requirement is to ensure that no packets are transmitted unless they are protected by IPSec.	UCR 2008: 5.3.5.3.8 (22.2)		X	EI-Softphone Conditional –WLAS/WAB Table E-13, Test Case 62
423	If RFC 4301 is supported, the device under test shall not support the mixing of IPv4 and IPv6 in a security association.	UCR 2008: 5.3.5.3.8 (22.3)		X	EI-Softphone Conditional –WLAS/WAB Table E-13, Test Case 63
424	If RFC 4301 is supported, the device under test's security association database (SAD) cache shall have a method to uniquely identify a SAD entry. Note: The concern is that a single SAD entry will be associated with multiple security associations. RFC 4301, Section 4.4.2, describes a scenario where this could occur.	UCR 2008: 5.3.5.3.8 (22.4)		X	EI-Softphone Conditional –WLAS/WAB Table E-13, Test Case 64
425	If RFC 4301 is supported, the device under test shall be capable of correlating the Differentiated Services Code Point (DSCP) for a VVoIP stream to the security association in accordance with UCR 2008, Section 5.3.2, Assured Services Requirements and Section 5.3.3, Network Infrastructure End-to-End Performance Requirements, plain text DSCP plan. For a more detailed description of the requirement, please see Section 4-1 of RFC 4301, *Security Architecture for the Internet Protocol.*	UCR 2008: 5.3.5.3.8 (22.5)		X	EI-Softphone Conditional –WLAS/WAB Table E-13, Test Case 65
426	If RFC 4301 is supported, the device under test shall implement IPSec to operate with both integrity and confidentiality.	UCR 2008: 5.3.5.3.8 (22.6)		X	EI-Softphone Conditional –WLAS/WAB Table E-13, Test Case 66
427	If RFC 4301 is supported, the device under test shall be capable of enabling and disabling the ability of the device to send an ICMP message informing the sender that an outbound packet was discarded.	UCR 2008: 5.3.5.3.8 (22.7)		X	EI-Softphone Conditional –WLAS/WAB Table E-13, Test Case 67
428	If an ICMP outbound packet message is allowed, the device under test shall be capable of rate limiting the transmission of ICMP Responses.	UCR 2008: 5.3.5.3.8 (22.7.1)		X	EI-Softphone Conditional –WLAS/WAB Table E-13, Test Case 68
429	If RFC 4301 is supported, the device under test shall be capable of enabling or disabling the propagation of the Explicit Congestion Notification (ECN) bits.	UCR 2008: 5.3.5.3.8 (22.8)		X	EI-Softphone Conditional –WLAS/WAB Table E-13, Test Case 69

ID	Requirement	Reference	IO	IA	Remarks
		IPv6 Requirements Applicable to Wireless Components			
430	If RFC 4301 is supported, the device under test's Security Policy Database (SPD) shall have a nominal, final entry that discards anything unmatched.	UCR 2008: 5.3.5.3.8 (22.9)		X	EI-Softphone Conditional –WLAS/WAB Table E-13, Test Case 70
431	If RFC 4301 is supported, and the device under test receives a packet that does not match any SPD cache entries and the device determines it should be discarded, the device shall log the event and include the date/time, Security Parameter Index (SPI), if available, IPSec protocol, if available, source and destination of the packet, and any other selector values of the packet.	UCR 2008: 5.3.5.3.8 (22.10)		X	EI-Softphone Conditional –WLAS/WAB Table E-13, Test Case 71
432	If RFC 4301 is supported, the device under test should include a management control to allow an administrator to enable or disable the ability of the system to send an Internet Key Exchange (IKE) notification of INVALID_SELECTORS.	UCR 2008: 5.3.5.3.8 (22.11)		X	EI-Softphone Conditional –WLAS/WAB Table E-13, Test Case 72
433	If RFC 4301 is supported, the device under test shall support the Encapsulating Security Payload (ESP) Protocol in accordance with RFC 4303.	UCR 2008: 5.3.5.3.9 (22.12)		X	EI-Softphone Conditional –WLAS/WAB Table E-13, Test Case 73
434	If RFC 4303 is supported, the device under test shall be capable of enabling anti-replay.	UCR 2008: 5.3.5.3.9 (22.12.1)		X	EI-Softphone Conditional –WLAS/WAB Table E-13, Test Case 74
435	If RFC 4303 is supported, the device under test shall check as its first check after a packet has been matched to its SA whether the packet contains a Sequence Number that does not duplicate the Sequence Number of any other packet received during the life of the security association.	UCR 2008: 5.3.5.3.9 (22.12.2)		X	EI-Softphone Conditional –WLAS/WAB Table E-13, Test Case 75
436	If RFC 4301 is supported, the device under test shall support the cryptographic algorithms as defined in RFC 4308 for Suite Virtual Private Network (VPN)-B.	UCR 2008: 5.3.5.3.9 (22.13)		X	EI-Softphone Conditional –WLAS/WAB Table E-13, Test Case 76
437	If RFC 4301 is supported, the device under test shall support the use of AES-CBC with 128-bits keys for encryption.	UCR 2008: 5.3.5.3.9 (22.13.1)		X	EI-Softphone Conditional –WLAS/WAB Table E-13, Test Case 77
438	If RFC 4301 is supported, the device under test shall support the use of HMAC-SHA1- 96 for (Threshold) and AES-XCBC-MAC-96 (FY2010).	UCR 2008: 5.3.5.3.9 (22.13.2)		X	EI-Softphone Conditional –WLAS/WAB Table E-13, Test Case 78
439	If RFC 4301 is supported, the device under test shall support IKE Version 1 (IKEv1) (Threshold) as defined in RFC 2409, and IKE Version 2 (IKEv2) (FY2010) as defined in RFC 4306. Note: Internet Key Exchange version 1 (IKEv1) requirements are found in UCR 2008, Section 5.4, Information Assurance.	UCR 2008: 5.3.5.3.9 (22.14)		X	EI-Softphone Conditional –WLAS/WAB Table E-13, Test Case 79

ID	Requirement	Reference	IO	IA	Remarks
IPv6 Requirements Applicable to Wireless Components
440	If the device under test supports IKEv2, it shall be capable of configuring the maximum User Datagram Protocol (UDP) message size.	UCR 2008: 5.3.5.3.9 (22.14.1) (Conditional)		X	All Table E-13, Test Case 80
441	If IKEv2 is supported, the device under test shall support the use of the ID_IPv6_ADDR and ID_IPV4_ADDR Identification Type.	UCR 2008: 5.3.5.3.9 (22.14.2) (Conditional)		X	All Table E-13, Test Case 81
442	If the device under test supports IKEv2, the device shall be capable of ignoring subsequent SA setup response messages after the receipt of a valid response.	UCR 2008: 5.3.5.3.9 (22.14.3) (Conditional)		X	All Table E-13, Test Case 82
443	If the device under test supports IKEv2, the device shall be capable of sending a Delete payload to the other end of the security association.	UCR 2008: 5.3.5.3.9 (22.14.4) (Conditional)		X	All Table E-13, Test Case 83
444	If the device under test supports IKEv2, the device shall reject initial IKE messages unless they contain a Notify payload of type COOKIE.	UCR 2008: 5.3.5.3.9 (22.14.5) (Conditional)		X	All Table E-13, Test Case 84
445	If the device under test supports IKEv2, the device shall close a SA instead of rekeying when its lifetime expires if there has been no traffic since the last rekey.	UCR 2008: 5.3.5.3.9 (22.14.6) (Conditional)		X	All Table E-13, Test Case 85
446	If the system supports IKEv2, the system shall not use the Extensible Authentication Protocol (EAP) method for IKE authentication.	UCR 2008: 5.3.5.3.9 (22.14.7) (Conditional)		X	All Table E-13, Test Case 86
447	If the device under test supports IKEv2, the device shall limit the frequency to which it responds to messages on UDP port 500 or 4500 when outside the context of a security association known to it.	UCR 2008: 5.3.5.3.9 (22.14.8) (Conditional)		X	All Table E-13, Test Case 87
448	If the device under test supports IKEv2, the device shall not support temporary IP addresses or respond to such requests.	UCR 2008: 5.3.5.3.9 (22.14.9) (Conditional)		X	All Table E-13, Test Case 88
449	If the device under test supports IKEv2, the device shall support the IKEv2 cryptographic algorithms defined in RFC 4307.	UCR 2008: 5.3.5.3.9 (22.14.10) (Conditional)		X	All Table E-13, Test Case 89
450	If the device under test supports IKEv2, the device shall support the VPN-B Suite as defined in RFC 4308 and RFC 4869 (FY2010).	UCR 2008: 5.3.5.3.9 (22.14.11) (Conditional)		X	All Table E-13, Test Case 90
451	If RFC 4301 is supported, the device under test shall support extensions to the Internet IP Security Domain of Interpretation for the Internet Security Association and Key Management Protocol (ISAKMP) as defined in RFC 2407.	UCR 2008: 5.3.5.3.9 (22.15)		X	All Table E-13, Test Case 91
452	If RFC 4301 is supported, the device under test shall support the ISAKMP as defined in RFC 2408.	UCR 2008: 5.3.5.3.9 (22.16)		X	All Table E-13, Test Case 92

ID	Requirement	Reference	IO	IA	Remarks
IPv6 Requirements Applicable to Wireless Components
453	If the device under test supports the IPSec Authentication Header Mode, the device under test shall support the IP Authentication Header (AH) as defined in RFC 4302.	UCR 2008: 5.3.5.3.9 (22.17)		X	All Table E-13, Test Case 93
454	If RFC 4301 is supported, the device under test shall support manual keying of IPSec.	UCR 2008: 5.3.5.3.9 (22.18)		X	All Table E-13, Test Case 94
455	If RFC 4301 is supported, the device under test shall support the ESP and AH cryptographic algorithm implementation requirements as defined in RFC 4305 and RFC 4835 (FY10).	UCR 2008: 5.3.5.3.9 (22.19)		X	All Table E-13, Test Case 95
456	If RFC 4301 is supported, the device under test shall support the IKEv1 security algorithms as defined in RFC 4109.	UCR 2008: 5.3.5.3.9 (22.21)		X	All Table E-13, Test Case 96
457	The device under test shall comply with the Management Information Base (MIB) for IPv6 textual conventions and general group as defined in RFC 4293. Note: The requirements to support SNMPv3 are found in UCR 2008, Section 5.3.2.17.3.1.5, SNMP Version 2 and Version 3 Format Alarm messages, and UCR 2008, Section 5.4, Information Assurance.	UCR 2008: 5.3.5.3.10 (23)	X	X	WLAS/WAB Table E-13, Test Case 97 TP IO-38
458	If the device under test performs routing functions, the device shall support the SNMP management framework as described in RFC 3411.	UCR 2008: 5.3.5.3.10 (23.1)		X	WLAS/WAB Table E-13, Test Case 98
459	If the device under test performs routing functions, the device shall support SNMP message processing and dispatching as described in RFC 3412.	UCR 2008: 5.3.5.3.10 (23.2)		X	WLAS/WAB Table E-13, Test Case 99
460	If the device under test performs routing functions, the device shall support the SNMP applications as described in RFC 3413.	UCR 2008: 5.3.5.3.10 (23.3)		X	WLAS/WAB Table E-13, Test Case 100
461	The device under test shall support the ICMPv6 MIBs as defined in RFC 4293.	UCR 2008: 5.3.5.3.10 (24)	X	X	WLAS/WAB Table E-13, Test Case 101 TP IO-39
462	The device under test shall support the Transmission Control Protocol (TCP) MIBs as defined in RFC 4022.	UCR 2008: 5.3.5.3.10 (25)	X	X	WLAS/WAB Table E-13, Test Case 102 TP IO-40
463	The device under test shall support the UDP MIBs as defined in RFC 4113.	UCR 2008: 5.3.5.3.10 (26)	X	X	WLAS/WAB Table E-13, Test Case 103 TP IO-41
464	If the device under test performs routing functions, the device shall support IP tunnel MIBs as described in RFC 4087.	UCR 2008: 5.3.5.3.10 (27)		X	WLAS/WAB Table E-13, Test Case 104
465	If the device under test performs routing functions, the device shall support the IP Forwarding MIB as defined in RFC 4292.	UCR 2008: 5.3.5.3.10 (28)		X	WLAS/WAB Table E-13, Test Case 105

ID	Requirement	Reference	IO	IA	Remarks
— IPv6 Requirements Applicable to Wireless Components					

ID	Requirement	Reference	IO	IA	Remarks
	IPv6 Requirements Applicable to Wireless Components				
466	If the device under test supports mobile users, the device shall support the Mobile IP Management MIBs as described in RFC 4295.	UCR 2008: 5.3.5.3.10 (29)		X	WLAS/WAB Table E-13, Test Case 106
467	If the device under test supports SNMP and supports routing functions, the device shall support the textual conventions for IPv6 flow labels as described in RFC 3595.	UCR 2008: 5.3.5.3.10 (30) (Conditional)		X	WLAS/WAB
468	If the device under test supports SNMP and IPSec, the device shall support the IPSec security policy database as described in RFC 4807.	UCR 2008: 5.3.5.3.10 (31)		X	WLAS/WAB Table E-13, Test Case 107
469	If the device under test uses Uniform Resource Identifiers (URIs), the device shall use the URI syntax described in RFC 3986.	UCR 2008: 5.3.5.3.10 (32)		X	All Table E-13, Test Case 108
470	If the device under test uses the Domain Name System (DNS), the device shall conform to RFC 3596 for DNS queries. Note: DNS is primarily used for NM applications.	UCR 2008: 5.3.5.3.10 (33)		X	All Table E-13, Test Case 109
471	For traffic engineering purposes, the bandwidth required per voice subscriber is calculated to be 110.0 Kbps (each direction) for each IPv6 call. This is based on G.711 (20 ms codec) with IP overhead (100 Kbps) resulting in a 250-byte bearer packet plus 10 Kbps for signaling, Ethernet Interframe Gap, and the SRTCP overhead. Based on overhead bits included in the bandwidth calculations, vendor implementations may use different calculations and hence arrive at slightly different numbers.	UCR 2008: 5.3.5.3.11 (34)	X		WLAS/WAB TP IO-42
472	The number of VoIP subscribers per link size for IPv6 is the same as for IPv4 and is defined in UCR 2008, Section 5.3.1, Assured Services Local Area Network Infrastructure Product Requirements.	UCR 2008: 5.3.5.3.11 (35)	X		WLAS/WAB TP IO-43
473	The number of video subscribers per link size for IPv6 is the same as for IPv4 and is defined in UCR 2008, Section 5.3.1, Assured Services Local Area Network Infrastructure Product Requirements.	UCR 2008: 5.3.5.3.11 (36)	X		WLAS/WAB TP IO-44
474	The device under test shall use the Alternative Network Address Types (ANAT) semantics for the Session Description Protocol (SDP) in accordance with RFC 4091 when establishing media streams from dual stacked appliances for AS-SIP signaled sessions.	UCR 2008: 5.3.5.3.12 (38)		X	WEI Table E-13, Test Case 111
475	The device under test shall prefer any IPv4 address to any IPv6 address when using ANAT semantics.	UCR 2008: 5.3.5.3.12 (38.1)	X		WEI TP IO-45

Table 3-1. Wireless Products Capability/Functional Requirements Table (continued)

ID	Requirement	Reference	IO	IA	Remarks
IPv6 Requirements Applicable to Wireless Components
476	The device under test shall place the SDP-ANAT option-tag in a required header field when using ANAT semantics in accordance with RFC 4092.	UCR 2008: 5.3.5.3.12 (38.2)		X	WEI Table E-13, Test Case 112
477	The device under test shall place the SDP-ANAT option-tag in a required header field when using ANAT semantics in accordance with RFC 4092.	UCR 2008: 5.3.5.3.12 (38.3)		X	WEI Table E-13, Test Case 113
478	The device under test shall place the SDP-ANAT option-tag in a required header field when using ANAT semantics in accordance with RFC 4092.	UCR 2008: 5.3.5.3.12 (38.3)		X	WEI Table E-13, Test Case 113
479	If the device under test is using AS-SIP and the <addrtype> is IPv6 and the <connection-address> is a unicast address, the system shall support generation and processing of unicast IPv6 addresses having the following formats: x:x:x:x:x:x:x:x (where x is the hexadecimal values of the eight 16-bit pieces of the address). Example: 1080:0:0:0:8:800:200C:417A:x:x:x:x:x:x :d.d.d.d (where x is the hexadecimal values of the six high-order 16-bit pieces of the address, and d is the decimal values of the four low-order 8-bit pieces of the address (standard IPv4 representation). Example: 1080:0:0:0:8:800:16.23.135.22	UCR 2008: 5.3.5.3.13 (39) (Conditional)	X		WEI TP IO-46
480	If the device under test is using AS-SIP, the system shall support the generation and processing of IPv6 unicast addresses using compressed zeros consistent with one of the following formats: • x:x:x:x:x:x:x:x format: 1080:0:0:0:8:800:200C:417A • x:x:x:x:x:x:d.d.d.d format: 1080:0:0:0:8:800:116.23.135.22 • compressed zeros: 1080::8:800:200C:417A.	UCR 2008: 5.3.5.3.13 (40) (Conditional)	X		WEI TP IO-47
481	If the device under test is using AS-SIP and the <addrtype> is IPv6 and the <connection-address> is a multicast group address (i.e., the two most significant hexadecimal digits are FF), the device shall support the generation and processing of multicast IPv6 addresses having the same formats as the unicast IPv6 addresses.	UCR 2008: 5.3.5.3.13 (41) (Conditional)	X		WEI TP IO-48

ID	Requirement	Reference	IO	IA	Remarks
IPv6 Requirements Applicable to Wireless Components
482	If the device under test is using AS-SIP and the <addrtype> is IPv6 and the <connection-address> is an IPv6 multicast group address, the multicast connection address shall not have a TTL value appended to the address as IPv6 multicast does not use TTL scoping.	UCR 2008: 5.3.5.3.13 (43) (Conditional)	X		WEI TP IO-49
483	If the device under test is using AS-SIP, the device shall support the processing of IPv6 multicast group addresses having the <number of address> field and may support generating the <number of address> field. This field has the identical format and operation as the IPv4 multicast group addresses.	UCR 2008: 5.3.5.3.13 (44) (Conditional)	X		WEI TP IO-50
484	The device under test shall support default address selection for IPv6 as defined in RFC 3484 (except for Section 2.1).	UCR 2008: 5.3.5.3.13 (46)		X	WEI - Softphone Table E-13, Test Case 115
485	If the device under test supports Remote Authentication Dial In User Service (RADIUS) authentication, the system shall support RADIUS in the manner defined in RFC 3162.	UCR 2008: 5.3.5.3.14 (47)		X	WLAS/WAB Table E-13, Test Case 116
486	If the device under test supports Mobile IP version 6 (MIPv6), the system shall provide mobility support as defined in RFC 3775.	UCR 2008: 5.3.5.3.14 (48)		X	WEI - Softphone Table E-13, Test Case 117
487	If the device under test supports Mobile IP version 6 (MIPv6), the system shall provide a secure manner to signal between mobile nodes and home agents in manner described in RFC 3776 and RFC 4877 (FY10).	UCR 2008: 5.3.5.3.14 (49)		X	WEI - Softphone Table E-13, Test Case 119
488	If the device under test supports network mobility (NEMO), the system shall support the function as defined in RFC 3963.	UCR 2008: 5.3.5.3.14 (51)		X	WEI - Softphone Table E-13, Test Case 120
489	The device under test shall support Differentiated Services as Described in RFC 2474 and RFC 5072 (FY10) for a voice and video stream.	UCR 2008: 5.3.5.3.14 (52)	X	X	All Table E-13, Test Case 121 TP IO-51
490	If the device under test acts as an IPv6 tunnel broker, the device shall support the function in the manner defined in RFC 3053.	UCR 2008: 5.3.5.3.14 (53)		X	WEI - Softphone Table E-13, Test Case 122
Other UCR Requirements
491	For NM, LAN products shall use Secure Shell 2 (SSH2). The SSH2 protocol shall be used instead of Telnet due to its increased security. The LAN products shall support RFC 4251 through RFC 4254 inclusive.	UCR 2008: 5.3.1.6 (1)		X	WLAS/WAB TP IA-

ID	Requirement	Reference	IO	IA	Remarks
		Other UCR Requirements			
492	For NM, LAN products shall use HyperText Transfer Protocol, Secure (HTTPS). HTTPS shall be used instead of HTTP due to its increased security, as described in RFC 2660. The LAN products shall support RFC 2818.	UCR 2008: 5.3.1.6 (2)		X	WLAS/WAB TP IA-
493	All LAN components shall be capable of providing status changes 99 percent of the time (with 99.9 percent as an Objective Requirement) by means of an automated capability in NRT.	UCR 2008: 5.3.1.6.3		X	WLAS/WAB TP IA-
494	All LAN components shall be capable of providing SNMP alarm indications to an NMS. Alarms shall be reported as TRAPs via SNMP in NRT. More than 99.95 percent of alarms shall be reported in NRT. NRT is defined as within 5 seconds of detecting the event, excluding transport time.	UCR 2008: 5.3.1.6.4		X	WLAS/WAB TP IA-
		Wireless STIGs			
495	The device under test shall support MAC address filtering.	Wireless STIG WIR0160: CAT III 2.2.3.3		X	All TP IA-
496	The device under test shall support VLANs.	Wireless STIG WIR0290: CAT II 2.2.3.8 2.2.1.2		X	All TP IA-
497	The device under test shall support disabling SSID broadcast mode.	Wireless STIG WIR0150: CAT II		X	All TP IA-
498	SSIDs not set to default.	Wireless STIG, WIR0105: CAT III Wireless STIG, WIR0140: CAT III		X	All TP IA-